

VŠB – Technická univerzita Ostrava
Fakulta elektrotechniky a informatiky
Katedra informatiky

Formalizace základních procesů rámce ITIL pomocí metody BPM

Basic Processes of the ITIL Framework and Their Formalization
by the BPM Method

2010

Bc. Jakub Janiš

Prohlašuji, že jsem tuto diplomovou práci vypracoval samostatně.

Uvedl jsem všechny literární prameny a publikace, ze kterých jsem čerpal.

Velmi rád bych poděkoval Ing. Štěpánu Kuchařovi za vedení diplomové práce, také za jeho odbornou pomoc, konzultace, cenné rady a připomínky při zpracování této práce.

Abstrakt

Tato diplomová práce se zabývá rámcem ITIL v3, který se stal mezinárodně uznávaným standardem v oblasti správy IT služeb. Metodologický rámec ITIL vychází z nejlepších zkušeností profesionálů z celého světa a v současné době je trendem v řízení služeb v mnoha organizacích, jejichž byznys aktivity jsou postaveny na informačních technologiích. Práce popisuje významná specifika rámce, postupně prochází a vysvětluje jednotlivé fáze životního cyklu služby a příslušné procesy, které jsou důležité pro kvalitní dodávku a podporu IT služeb.

Pro efektivní zavedení principů a technik rámce ITIL v organizaci je důležité přesně specifikovat a formalizovat procesy, které se podílejí na řízení IT služeb. Procesy je zpravidla nutné přizpůsobit kultuře, filozofii, zvykům a prostředí konkrétní organizace. Diplomová práce se rovněž věnuje možnostem formalizace byznys procesů založeným na precizně definované metodě Petriho sítě. Součástí práce jsou ukázky modelů některých základních procesů ITIL v3 vytvořené pomocí metody BPM.

Klíčová slova

ITSM, správa IT služeb, ITIL, Information Technology Infrastructure Library, BPM, Petriho síť, Workflow, Workflow síť, BPM, Business Process Modeling, formalizace byznys procesů

Abstract

This master thesis deals with the ITIL v3 framework, which has become an internationally accepted standard in the area of IT Service Management. The methodological ITIL framework is based on best practices of professionals from the whole world and it is considered to be a current trend in IT service management in many organizations the business activities of which build upon information technologies. The thesis introduces significant particulars of the framework, goes through every single phase of service lifecycle and describes proper processes that are important to deliver and support IT services in a high quality.

Accurate specification and formalization of processes that are involved in IT Service Management form an integral part of an efficient implementation of appropriate ITIL principles and techniques in an organisation. It is necessary to adapt the processes to business culture, philosophy, customs and environment. The thesis also deals with business process formalization methods based on precisely defined technique of Petri Nets. The work includes models of some essential ITIL v3 processes created by the BPM method.

Keywords

ITSM, IT Service Management, ITIL, Information Technology Infrastructure Library, Petri Nets, Workflow, Workflow Nets, BPM, Business Process Modeling, business process formalization

Seznam použitých symbolů a zkratek

ASL	Application Services Library
AST	Agreed Service Time
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BPM	Business Process Modeling
BPMN	Business Process Modeling Notation
BPO	Business Process Outsourcing
CAB	Change Advisory Board
CCTA	The Central Computer and Telecommunications Agency
CFIA	Component Failure Impact Analysis
CI	Configuration Item
CMDB	Configuration Management Database
CMIS	Capacity Management Information System
CMS	Configuration Management System
COBIT	The Control Objectives for Information and related Technology
CRM	Customer Relationship Management
CS	Change Schedule
CSF	Critical Success Factor
CSI	Continual Service Improvement
DIKW	Data-to-Information-to-Knowledge-to-Wisdom
DML	The Definitive Media Library
ELS	Early Life Support
EPC	Event-driven Process Chain
ERP	Enterprise Resource Planning
FTA	Fault Tree Analysis
ICT	Information and Communication Technologies
ISM	Information Security Management
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library

ITSCM	IT Service Continuity Management
ITSM	Information Technology Service Management
KEDB	Known Error Database
KPI	Key Performance Indicator
MOF	Microsoft Operations Framework
MTBF	Mean Time Between Failures
MTBSI	Mean Time Between Service Incidents
MTRS	Mean Time to Restore Service
OGC	Office of Government Commerce
OLA	Operational Level Agreement
OLA	Operational Level Agreement
PIR	Post Implementation Review
PN	Petri Nets
RA	Risk Analysis
RAD	Rapid Application Development
RFC	Request for Change
ROI	Return On Investment
SACM	Service Asset and Configuration Management
SCD	Supplier and Contract Database
SDP	Service Design Package
SFA	Service Failure Analysis
SKMS	Service Knowledge Management System
SLA	Service Level Agreement
SLM	Service Level Management
UML	Unified Modeling Language
VBF	Vital Business Functions
WfMS	Workflow Management System

Obsah

1	Úvod.....	2
2	Obecně o ITILu.....	3
2.1	Správa IT služeb bez zavedeného standardu.....	3
2.2	Co je ITIL?.....	3
2.3	Stručně z historie.....	4
2.4	Charakteristické znaky rámce ITIL.....	5
3	ITIL v3.....	7
3.1	Service Strategy	8
3.1.1	Service Portfolio Management.....	9
3.1.2	Financial Management.....	10
3.1.3	Demand Management	10
3.2	Service Design	11
3.2.1	Service Level Management.....	13
3.2.2	Service Catalogue Management.....	14
3.2.3	Capacity Management.....	15
3.2.4	Availability Management.....	16
3.2.5	Information Security Management	18
3.2.6	IT Service Continuity Management.....	19
3.2.7	Supplier Management	20
3.3	Service Transition	21
3.3.1	Transition Planning and Support.....	22
3.3.2	Service Asset and Configuration Management.....	23
3.3.3	Change Management.....	25
3.3.4	Release and Deployment Management.....	27
3.3.5	Service Validation and Testing	31
3.3.6	Knowledge Management	33
3.3.7	Evaluation	35
3.4	Service Operation.....	36
3.4.1	Event management.....	37
3.4.2	Incident Management.....	39

3.4.3	Problem Management	42
3.4.4	Request Fulfilment	45
3.4.5	Access Management.....	46
3.5	Continual Service Improvement	49
3.5.1	Service Measurement	49
3.5.2	Continual Service Improvement Process	49
3.5.3	Service Reporting.....	51
4	Formální zápis byznys procesů pomocí Petriho sítí.....	52
4.1	Petriho sítě.....	52
4.1.1	Klasické Petriho sítě.....	52
4.1.2	Rozšíření klasických Petriho sítí	53
4.2	Možnosti formálního zápisu procesů pomocí Petriho sítí	55
4.2.1	Workflow sítě.....	55
4.2.2	Business Process Modeling.....	61
5	Formalizace základních procesů ITIL v3 metodou BPM	64
5.1	Ukázkové modely procesu Incident Management	64
5.1.1	Funkční model.....	64
5.1.2	Objektový model.....	65
5.1.3	Koordinační model.....	66
6	Závěr	70
7	Literatura.....	71
8	Seznam příloh	73

Seznam obrázků

Obr. 1: Princip procesního managementu.....	5
Obr. 2: Koloběh zákaznický orientovaného přístupu – The Service Profit Chain	6
Obr. 3: Model rámce ITIL v3 znázorňující životní cyklus IT služby [7].....	7
Obr. 4: Portfolio služeb (Service Portfolio) [9]	9
Obr. 5: Byznys katalog služeb a technický katalog služeb [9].....	14
Obr. 6: Metriky dostupnosti služby v rámci životního cyklu incidentů [9]	17
Obr. 7: Souvislost The Definite Media Library s CMDB [11]	24
Obr. 8: Mapování testovacích aktivit na etapy vývoje služby pomocí V-modelu [11].....	32
Obr. 9: Struktura DIKW – spojení dat do souvislostí a umožnění lepšího rozhodování [11].....	34
Obr. 10: Oddělení důležitých příčin od triviálních pomocí Paretovy analýzy [12]	43
Obr. 11: Přechod od výskytu chyby v IT infrastruktuře k vyřešenému problému	44
Obr. 12: Spolupráce Incident a Problem Managementu	45
Obr. 13: Princip procesu plnění uživatelských požadavků	46
Obr. 14: Continual Service Improvement Process [13]	51
Obr. 15: Příklad modelování jednoduchého procesu pomocí Petriho sítí	53
Obr. 16: Tři dimenze konceptu workflow.....	55
Obr. 17: Řídící konstrukce workflow sítí.....	57
Obr. 18: Typy spouštěčů úloh ve workflow sítích (triggers)	58
Obr. 19: Ukázka modelování jednoduchého procesu pomocí workflow sítí	60
Obr. 20: Příklad funkčního modelu metody BPM	61
Obr. 21: Příklad objektového modelu metody BPM.....	62
Obr. 22: Příklad koordinačního modelu metody BPM	63
Obr. 23: Funkční model procesu Incident Management - spolupráce s ostatními procesy.....	64
Obr. 24: Funkční model procesu Incident Management – vstupy, výstupy, aj.	65
Obr. 25: Objektový model procesu Incident Management	66
Obr. 26: Koordinační model procesu Incident Management	68
Obr. 27: Koordinační model podprocesu „Řešení incidentu“	69

1 Úvod

V mnoha organizacích se neustále prohlubuje závislost podnikových procesů na informačních a komunikačních technologiích (ICT), a na službách, které tyto technologie poskytují. Pro správné fungování IT služeb je nutné řídit nejen jednotlivé komponenty ICT infrastruktury, ale i samotné IT služby. Řízením IT služeb se zabývá disciplína, která se nazývá IT Service Management (ITSM), a jedním z nejznámějších a nejuznávanějších přístupů v oblasti ITSM je rámec ITIL. ITIL je knihovnou, která vychází z nejlepších praktických zkušeností a je šířena prostřednictvím množství školení, konzultací, knih a dalších médií.

Diplomová práce je rozdělena na čtyři hlavní části. První část nazvaná „Obecně o ITILu“ zdůrazňuje důležitost zavedeného standardu pro správu IT služeb v organizaci a seznamuje čtenáře se základní podstatou a obecnými rysy rámce ITIL, který se stal mezinárodně uznávaným standardem pro správu IT služeb. V této kapitole je také stručně nastíněn historický vývoj rámce.

Další kapitola, tvořící značnou část diplomové práce, se nazývá „ITIL v3“ a zabývá se třetí verzí knihovny ITIL, která se skládá celkem z pěti publikací. Charakteristickou vlastností dosud nejnovější verze knihovny je její zaměření na životní cyklus IT služeb, který sestává z pěti fází. Každá publikace knihovny tedy reprezentuje jednu fázi. Kapitola se zabývá popisem jednotlivých etap životního cyklu služby, náležitých procesů, funkcí a aktivit, které jsou stěžejní v rámci efektivního řízení IT služeb. Přestože jsou procesy odděleny do samostatných podkapitol, nejsou opomíjeny jejich vzájemné návaznosti a souvislosti. Práce klade velký důraz zejména na etapu návrhu služby, přechodu služby do živého prostředí a fázi operativní. V kapitole jsou rovněž zmíněny některé odlišnosti ITIL v3 od předchozí verze tohoto rámce.

Následující dvě části diplomové práce se věnují formalizaci procesů ITIL v3 prostřednictvím syntakticky i sémanticky precizně definované metody Petriho sítí. Jsou zde vysvětleny klíčové principy, na kterých je základní forma Petriho sítí postavena, a také jsou uvedeny způsoby rozšíření této techniky, které ji umožňují přizpůsobit modelování byznys procesů. Práce se dále zabývá metodou Workflow sítí, které vznikají mapováním Petriho sítí na workflow. Následně je popsána druhá specializovaná metoda pro formalizaci, analýzu a simulaci byznys procesů, zvaná Business Process Modeling (BPM). V samotném závěru diplomové práce je možno shlédnout ukázky modelů jednoho ze základních procesů rámce ITIL v3, vytvořené pomocí metody BPM a nástroje BP Studio. Modely dalších procesů nalezneme v přílohách této diplomové práce.

2 Obecně o ITILu

2.1 Správa IT služeb bez zavedeného standardu

V podniku, ve kterém není zaveden žádný standard pro správu IT služeb, sice obvykle existuje mechanismus pro řízení jednotlivých komponent ICT infrastruktury, nicméně, za řízení samotných IT služeb nebývá odpovědný nikdo. Také si málokdo uvědomuje, že IT neposkytuje služby pouze externím zákazníkům ale i ostatním útvarům organizace, které se stávají jeho interními zákazníky. Absence standardu pro poskytování služeb a nedostatečná správa IT služeb mohou vést k mnoha problémům, uvedme si některé z nich: [1]

- ❑ IT oddělení nemusí plně porozumět potřebám zákazníků a uživatelů. Stejně tak uživatelé nemusejí chápat zákonitosti fungování IT infrastruktury. Následkem toho IT neposkytuje takové služby, jaké si přejí zákazníci.
- ❑ IT oddělení je považováno za nezávislé oddělení, a proto může váznout komunikace a spolupráce s ostatními odděleními podniku.
- ❑ V rámci vývoje, zavádění a podpory služeb nemá personál k dispozici dostatečné a relevantní informace o prvcích IT infrastruktury a dalších okolnostech důležitých pro provoz služby. Správné fungování IT je často závislé na individuálních znalostech a schopnostech jednotlivých specialistů.
- ❑ V podniku neexistuje přehled o nákladech vynaložených na poskytování jednotlivých služeb a organizace není schopna náklady patřičně odůvodnit. Je pro ni obtížné správně posoudit kvalitu poskytovaných služeb a vyčíslit jejich hodnotu.
- ❑ Často se stává, že jsou nejprve nakoupeny produkty a technologie, aby se zvládly především technické záležitosti. Personál, partneři a procesy jsou pak přizpůsobovány technice a jejím omezením.
- ❑ Organizace postrádá preventivní opatření proti výpadkům služeb. To znamená, že problémy spojené s poskytováním služeb se řeší až v momentě, kdy nastanou. Většinou neexistuje kvalitní mechanismus sloužící k průběžnému měření a zdokonalování IT služeb a procesů.

2.2 Co je ITIL?

ITIL (Information Technology Infrastructure Library) je označení rámce pro správu IT služeb ve firmě nebo organizaci. Správa IT služeb (ITSM – IT Service Management) se nezabývá pouze technickými aspekty informatiky, ale jejím primárním úkolem je, aby veškeré investice do informatiky a její provoz byly sladěny s cíli organizace a jejími dlouhodobými záměry. Na jejím vytvoření spolupracovala řada společností a vládních organizací, v současné době je spravována organizací OGC (Office of Government Commerce).

Rámec ITIL je souborem doporučení, která vycházejí z nejlepší praxe (Best Practices) a především nám dává odpověď na otázku, jak nastavit procesy a role v organizaci, a odhaluje další potřebné zásady a typy sloužící pro efektivní správu informatiky v organizaci. Je nutno zmínit, že ITIL nám nepřináší podrobné návody ani předpřipravené toky činností, které by stačilo jen nasadit v organizaci. Slouží spíše jako podklad pro definici podnikového procesu. Zaměřuje se na klíčové principy, hlavní aktivity a kritéria pro hodnocení a kontrolu kvality.

V knihovně nalezneme také doporučení, jaké služby by měl pro daný proces poskytovat podpůrný softwarový nástroj, čímž se pracovníkům IT zjednoduší výběr a nákup podpůrné technologie. Jednoduše řečeno, ITIL nám sděluje, co se má v organizaci udělat, zatímco způsob provedení (tedy jak se to má udělat) už závisí na konkrétní organizaci, která ITIL implementuje, na její interní kultuře, velikosti atd. [2]

Díky knihovně ITIL můžeme lépe pochopit, k čemu jednotlivé podnikové procesy slouží, jaké existují vazby mezi procesy, jaké role by se měly podílet na procesu, popř. jaké parametry by měl proces mít. Kromě návodu, jak dobře řídit IT služby, knihovna nabízí také způsoby vylepšování IT služeb. Vzhledem k tomu, že mechanismy pro zlepšování činností jsou obsaženy přímo v jednotlivých procesech, implementace procesů podle ITIL v organizaci zaručuje průběžné zvyšování kvality a produktivity. ITIL je rozvinuta do takových detailů, že je využitelná pro řešení podpory jak u organizací veřejného sektoru, tak u soukromých společností.

Metodika je podporována celou řadou softwarových nástrojů a opírá se o kvalitní standardy, jako jsou normy řady ISO 9000. Jedná se o normy, které vydává Mezinárodní organizace pro normalizaci (ISO) a popisují systém managementu jakosti. Stěžejní je zejména norma 9001:

Norma ISO 9001 specifikuje požadavky na systém managementu jakosti pro případ, že organizace musí prokázat svoji schopnost poskytovat produkty, které splňují požadavky zákazníka a aplikovatelné požadavky předpisů, a že má v úmyslu zvýšit spokojenost zákazníků. [3]

2.3 Stručně z historie

Návrh na vytvoření rámce se objevil poprvé v 80. letech 20. stol. Tehdy britská vláda dospěla k závěru, že úroveň a kvalita poskytovaných IT služeb byla nedostatečná. Proto organizace CCTA (The Central Computer and Telecommunications Agency), která je nyní nazývána OGC (Office of Government Commerce), dostala za úkol vyvinout rámec, který by přispěl k efektivnějšímu využití IT zdrojů v britské vládě i v soukromém sektoru.

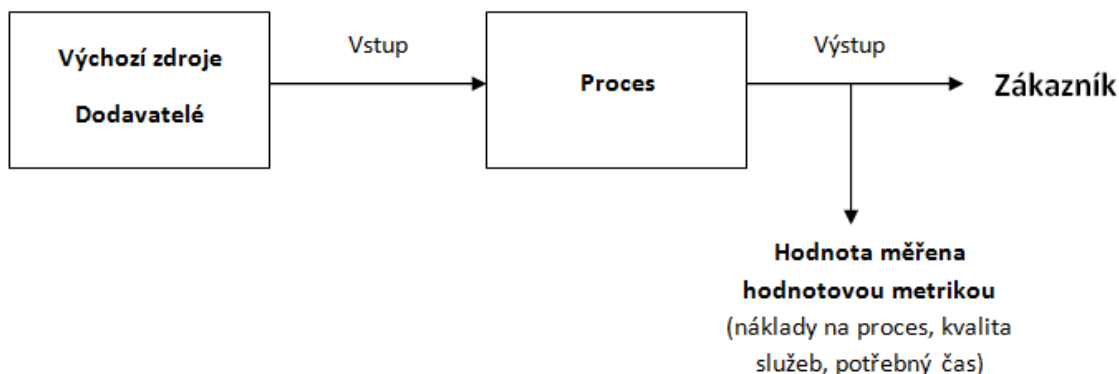
V 90. letech mnoho velkých organizací tento rámec přijalo a začalo jej naplno používat. ITIL se začal nesmírně rychle šířit a byl využíván ve spoustě vládních i nevládních organizací. Popularita knihovny ITIL v těchto letech rostla a měnila se spolu s vyvíjejícími se informačními technologiemi. Rovněž došlo k rozvoji mezinárodně uznávaných standardů, které souvisí se správou IT služeb, jako např. ISO (International Organization for Standards) nebo BS (British Standards). V roce 2000 použila firma Microsoft rámec ITIL jako základ pro vývoj Microsoft Operations Framework (MOF). MOF není považován za náhradu ITIL, ale o konkrétní implementaci nejlepších praktik pro organizace využívající softwarové IT řešení převážně na platformě Microsoft.

Roku 2001 byla vydána nová verze knihovny a to verze 2. Publikace týkající se podpory a dodávky služeb byly přetvořeny do stručnější a lépe použitelné formy. Během následujících let se rámec stal světově nejpoužívanějším přístupem pro správu IT služeb. V roce 2007 byla publikována už třetí verze ITIL, která druhou verzi rozšiřuje a doplňuje ji o nové procesy, další praktiky a poznatky. Klade také větší důraz na získání hodnot pro samotný byznys. [4]

2.4 Charakteristické znaky rámce ITIL

Procesní řízení

Jedním z nejvýznamnějších charakteristických rysů rámce ITIL je procesně orientovaný přístup k řízení IT služeb (viz Obr. 1). Proto se v ITIL objevují procesy, jejich vlastníci, role a odpovědnosti. Procesem zde rozumíme logický sled úloh - proceduru, která transformuje daný vstup na určitý výstup, přičemž plnění jednotlivých úloh v procesu je zajištěno úlohami s jasně definovanými odpovědnostmi. [5]



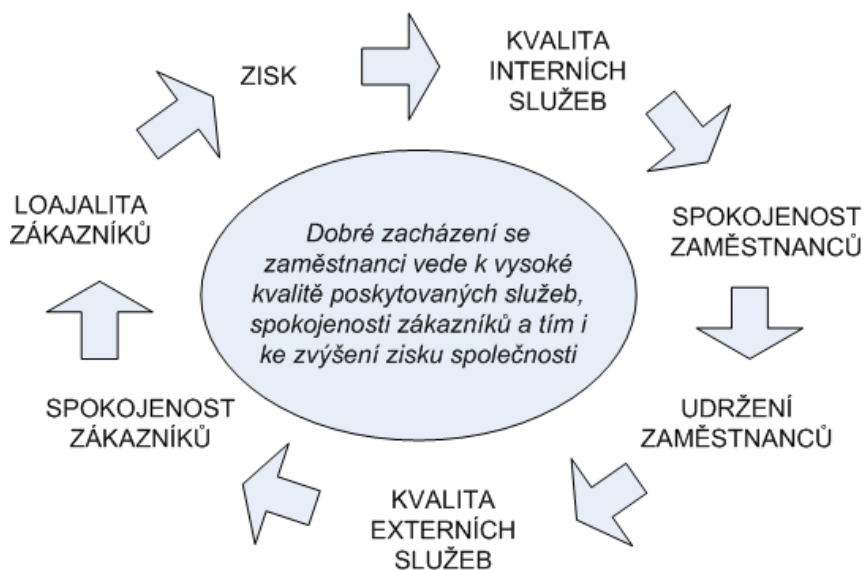
Obr. 1: Princip procesního managementu

Tento přístup má výhodu v tom, že je nezávislý na funkční struktuře společnosti. Procesní řízení je založeno na týmové spolupráci a důležitý je především výsledek procesu. Vlastníci procesů, tedy osoby, které jsou odpovědné za proces, mají k dispozici výkonnostní ukazatele vypovídající o účinnosti a efektivnosti procesů. Díky měření a monitorování je proto možno procesy neustále vylepšovat. Velkou výhodou je, že zaměstnanci mohou navazovat přímý vztah se zákazníkem a jejich hlavním záměrem není splnění přiřazených příkazů, ale v první řadě uspokojení požadavků zákazníků. A to je jeden z dalších rysů rámce.

Zákaznický orientovaný přístup

Dalším charakteristickým znakem a zároveň principem IT service managementu podle ITIL je zákaznický orientovaný přístup. Základem je Service Profit Chain model (viz Obr. 2). Jedná se o model, který zajišťuje, že veškeré aktivity mají za cíl přinést přidanou hodnotu pro zákazníka (a to interního i externího). Pokud nějaká aktivita nepřináší přidanou hodnotu pro zákazníka, považujeme ji za nadbytečnou.

Model znázorňuje vztah mezi ziskovostí organizace, loajalitou zákazníků a jejich spokojeností, oddaností a produktivitou zaměstnanců. Z následujícího diagramu vyplývá, že zisk a růst jsou primárně stimulovány loajalitou zákazníků. Loajalita je přímým následkem spokojenosti zákazníků a ta je ovlivněna zejména hodnotou a kvalitou služeb poskytovaných společností. Hodnota služeb je vytvářena v závislosti na spokojených, produktivních a oddaných pracovnících. Loajalita zákazníků je tedy podstatný faktor zvyšující zisk a růst organizace. [6]



Obr. 2: Koloběh zákaznický orientovaného přístupu – The Service Profit Chain

Nezávislost na platformě

Zásadní charakteristikou, která by měla být rovněž zmíněna, je nezávislost na platformě. Nezáleží na tom, jakou informační a komunikační infrastrukturu je potřeba řídit a spravovat. Stejně tak nezáleží ani na tom, jaké služby jsou na této infrastruktuře poskytovány. ITIL v tomto ohledu dává organizaci dostatečnou svobodu - definuje pouze hranice, pravidla a důležité vazby. Rámec je možné použít v jakékoliv firmě, která podniká ve službách, dokonce i mimo oblast ICT.

Jednoznačná terminologie

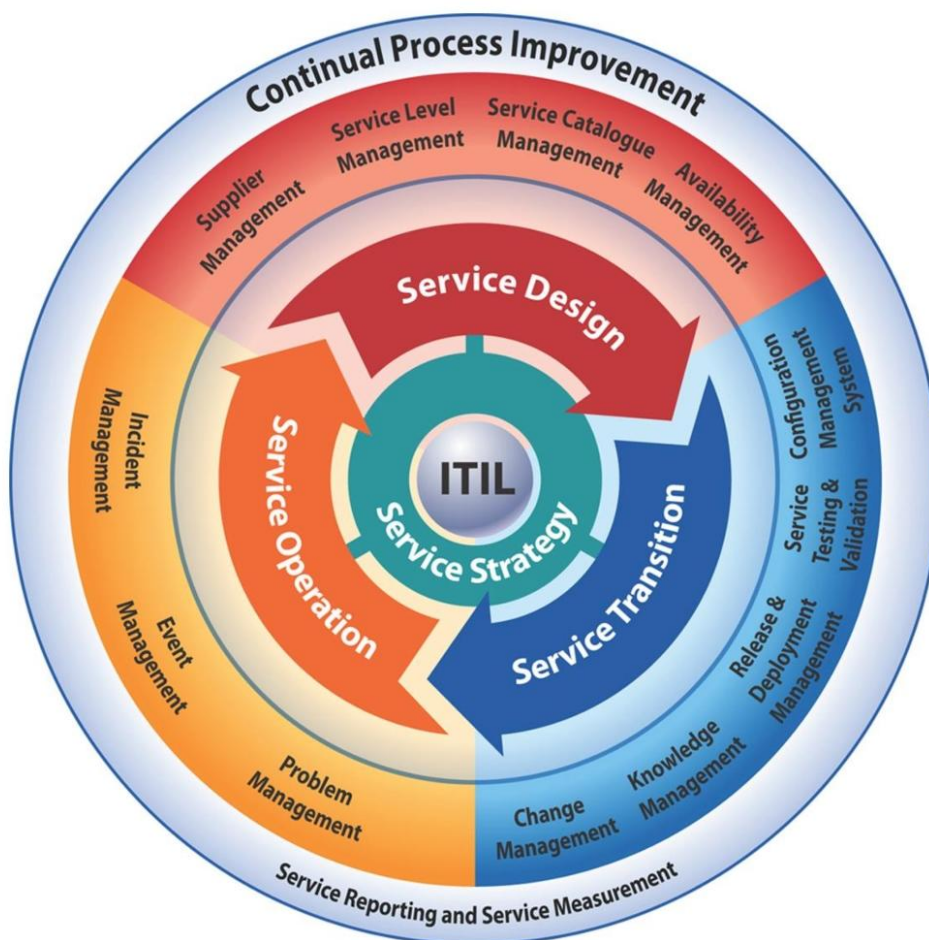
Jedním z největších problémů v organizaci může být špatná komunikace. Ta může nastat z různých důvodů a jedním z nich je chabá a nekonzistentní terminologie. ITIL proto definuje jednoznačnou terminologii, která usnadňuje komunikaci nejen uvnitř organizace, ale i s obchodními partnery.

Veřejná dostupnost

Knihovna je veřejně dostupná a to znamená, že každý má možnost knihy zakoupit a procesy ITSM podle ITIL ve svém podniku implementovat. Tato skutečnost mimo jiné přispěla k jejímu rychlému celosvětovému rozšíření.

3 ITIL v3

Zatímco publikace rámce ITIL v2 byly rozděleny do určitých logických celků, seskupovaly příbuzné procesy z hlediska určitého pohledu na správu IT a služeb, ITIL v3 se zaměřuje na životní cyklus služeb a všechny procesy jsou proto organizovány do několika fází vývoje služby. Třetí verze rámce nám rovněž poskytuje přehled nad tím, jak jsou jednotlivé komponenty správy služeb propojeny. Životní cyklus služeb se skládá celkem z pěti fází a každá publikace popisuje jednu z těchto fází: Service Strategy, Service Design, Service Transition, Service Operation, Continual Service Improvement (viz Obr. 3).



Obr. 3: Model rámce ITIL v3 znázorňující životní cyklus IT služby [7]

Jednotlivé fáze a jejich procesy jsou popsány v následujících kapitolách.

V předchozích verzích rámce ITIL se často řešila otázka, jakým způsobem sjednotit byznys cíle s IT (Business and IT alignment). Přestože jsou byznys a IT součástí dané organizace, byly považovány za dvě separátní a odlišné funkce. V rámci ITIL v3 je role IT ještě více zdůrazněna a IT je chápáno jako integrovaná a nedílná součást byznysu, jelikož procesy a podpůrné technologie jsou neustále více propojeny a jsou na sobě tak závislé, že se staly neoddělitelnými (Business and IT integration).

3.1 Service Strategy

Úvodem této kapitoly bych rád podotknul, že tato část knihovny ITIL je zcela zaměřena na byznys, nikoliv na samotnou správu služeb nebo řízení informatiky při poskytování služeb. Kniha není primárně určena pro technické odborníky nebo vedoucí provozu IT, ale spíše pro ředitele informatiky, finanční ředitele nebo finanční analytiku. Z tohoto důvodu je v této kapitole popsán pouze stručný pohled na jádro problematiky, výklad nezachází do podrobných detailů.

Strategie služeb libovolného poskytovatele by měla být založena na myšlence, že zákazníci si nekupují produkty, nýbrž určitou formu uspokojení svých potřeb. Poskytovaná služba musí přinášet zákazníkovi dostatečnou hodnotu. Jinými slovy musí splňovat to, co od ní zákazník očekává. Aby bylo možné služby poskytovat, je nutné si nejprve uvědomit, kdo je stávajícím či potenciálním zákazníkem, jaké jsou potřeby zákazníků, co pro ně tyto potřeby znamenají, apod. Poskytovatel musí rozumět v širším kontextu aktuálním či potenciálním trhům.

Publikace Service Strategy tvoří jádro rámce ITIL v3, na kterém staví všechny další publikace a fáze vývoje služby. Strategie služeb napomáhá organizaci zajistit dlouhodobou prosperitu, a to především díky identifikaci několika stěžejních bodů:

- ☐ Jaké služby budou nabízeny
- ☐ Komu budou služby nabízeny
- ☐ Jaká je existující a potenciální konkurence na trhu
- ☐ Jakým způsobem bude vytvářena hodnota
- ☐ Jak budou zákazníci a všichni zainteresovaní vnímat a posuzovat hodnotu
- ☐ Jak efektivně přidělovat zdroje a prostředky v rámci portfolia služeb
- ☐ Jakým způsobem bude měřena kvalita a výkonnost služeb
- ☐ Jaké budou role a zodpovědnosti

Všechny tyto aspekty a mnoho dalších jsou součástí dlouhodobého strategického plánování společnosti. Můžeme zde zařadit i další faktory, kterými se publikace zabývá – SWOT analýza (analýza silných a slabých stránek společnosti, možných hrozeb a příležitostí), unikátnost na trhu, kritické faktory úspěchu (CSFs), návratnost investice, outsourcing služeb aj.

Během strategické fáze jsou formulovány základní strategické cíle, politiky, plány, a je nastíněna obecná vize a zaměření organizace.

Procesy fáze Service Strategy:

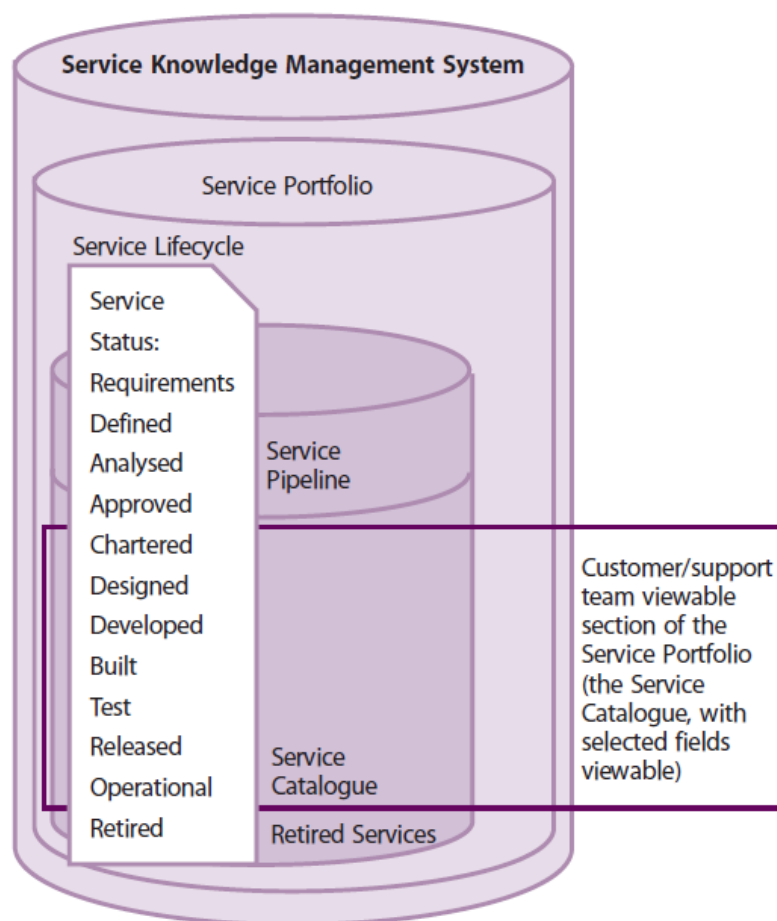
- ☐ Service Portfolio Management
- ☐ Financial Management
- ☐ Demand Management

Problematika strategie služeb a s ní související procesy jsou podrobně popsány v publikaci „Service Strategy“. [8]

3.1.1 Service Portfolio Management

Pro lepší kontrolu nad službami zavádí ITIL proces Service Portfolio Management, který poskytuje efektivní správu služeb během celého životního cyklu. Tento proces je užitečný zejména pro efektivní přidělení zdrojů, stanovení priorit, vytvoření cenových modelů, management rizik, apod. Zabývá se rovněž konkurenčními výhodami a nevýhodami služeb vůči jiným poskytovatelům a dalšími strategickými otázkami.

Základem pro správu služeb je tzv. Service Portfolio (Portfolio služeb) zahrnující komplexní a přesnou dokumentaci všech existujících či plánovaných služeb (viz Obr. 4). Dokumentace sestává z různých atributů služeb – popis služeb, priority, rizika, náklady, stanovování cen, aj. Portfolio udržuje také aktuální stav služby (např. definovaná, schválená, navržená, vytvořená, otestovaná, nasazená). Tyto všechny atributy jsou ohodnocovány v průběhu životního cyklu služby, počínaje strategickou analýzou až po vyřazení služby z produkčního prostředí. Portfolio služeb se skládá ze tří kategorií: Service Pipeline, Service Catalogue a Retired Services.



Obr. 4: Portfolio služeb (Service Portfolio) [9]

□ Service Pipeline (Připravované služby)

Service Pipeline je soubor služeb, které jsou plánovány, připravovány nebo se nacházejí ve stádiu vývoje, ale prozatím nejsou dostupné zákazníkům.

❑ Service Catalogue (Katalog služeb)

Service Catalogue je podmnožinou portfolia služeb, která je viditelná a přístupná zákazníkům. Katalog služeb obsahuje všechny služby, které byly schváleny a jsou připraveny k nasazení nebo už jsou zavedeny do provozu. Služby zveřejněné v katalogu si tedy může zákazník objednat, zakoupit a následně využívat. V rámci katalogu jsou udržovány některé důležité atributy služeb, jako např. popisy služeb, politiky, související dohody SLA, postupy při objednávání služeb, podmínky pro podporu služeb, stanovení cen za služby atd.

❑ Retired Services (Ukončené služby)

Služby, které již nejsou potřebné pro byznys, označujeme pojmem Retired Services. V této sekci se nacházejí služby, které byly nahrazeny jinými službami nebo služby, které již nejsou nákladově výhodné, a proto byl jejich provoz ukončen. Aby mohly být tyto služby identifikovány, provádí se periodická revize portfolia.

3.1.2 Financial Management

Vzhledem k zvyšujícímu se počtu uživatelů služeb, požadavkům na nové technologie a stále složitějším IT systémům dochází k rychlému růstu nákladů na IT služby. V důsledku toho může nastat situace, že organizace nejsou schopny prokázat a odůvodnit náklady vynaložené na vývoj nových služeb či vylepšování stávajících služeb. IT služby mohou být zákazníkem vnímány jako příliš drahé.

Finanční Management představuje nákladově efektivní správu všech IT aktiv a zdrojů potřebných k poskytování IT služby a podporuje organizaci v plánování a realizaci jejích byznys cílů. Správa financí umožňuje společnosti správně vyčíslit hodnotu poskytovaných služeb a hodnotu aktiv zajišťujících tyto služby. Zabývá se také návratností investic (Return On Investment - ROI). Finanční management zahrnuje proces sestavování rozpočtu (budgeting), který umožňuje předpovědět na určitou dobu množství financí nezbytných pro provoz služeb, porovnat predikované výlohy s aktuálními výdaji a zároveň snižovat riziko překročení výdajů. Součástí je také proces pro vedení účetnictví (accounting), který poskytuje správu financí vynaložených na poskytování služeb, kalkulaci nákladů za služby interním a externím zákazníkům, a pomáhá určit náklady potřebné pro změny.

3.1.3 Demand Management

Demand Management je procesem, jehož cílem je synchronizovat poptávku zákazníků s dodávkou služeb a předvídat a regulovat jejich odbyt. Jinými slovy, účelem procesu je pochopit a ovlivňovat poptávku a zároveň zajistit přiměřenou kapacitu pro naplnění požadavků zákazníků. Je samozřejmostí, že nadbytečná kapacita vede pouze k zvyšování nákladů, aniž by byla vytvářena patřičná hodnota pro zákazníka.

3.2 Service Design

Service Design je následující fází životního cyklu služby a jejím hlavním záměrem je návrh a vývoj služeb a souvisejících procesů pro jejich uvedení do produkčního prostředí. Je nutno zmínit, že návrh se vztahuje na nové i modifikované služby. Fáze se zabývá předcházením a minimalizací rizik, úsporami financí a času, posuzováním a vylepšováním kvality a efektivity služeb, podporou vývoje politik a standardů, a výrazně tak přispívá k dosažení obchodních cílů organizace a naplnění stávajících i budoucích potřeb zákazníků.

Návrh dobře fungujících a úspěšných IT služeb je založen na vytváření rovnováhy mezi funkcionalitou, dostupnými prostředky a časem. Prostředky zahrnují především finanční, technické a lidské zdroje. Jedná se o proces probíhající v rámci celého životního cyklu služeb.

Aby byla dosažena vysoká kvalita služeb s možností průběžného vylepšování, je důležité, aby byl návrh dobře strukturovaný a zároveň aby byl orientovaný na výsledky. Orientací na výsledky chápeme uspokojení všech potřeb zákazníků a uživatelů. Z tohoto důvodu se fáze zaměřuje na pět různých aspektů, které jsou nezbytné pro poskytování služeb:

- ☐ Návrh samotných IT služeb – specifikace funkčních požadavků, řízení prostředků a kapacity
- ☐ Portfolio služeb – informace o poskytovaných službách a jejich stavu, podpora procesů, zpřístupnění katalog služeb zákazníkům
- ☐ Architektura – architektura technologií (IT infrastruktura, aplikace, data) a managementu (personál, procesy, obchodní partneři)
- ☐ Procesy - využití norem, standardů, definice aktivit vstupů a výstupů, rolí a vlastníků procesů
- ☐ Měřicí nástroje a metriky – návrh měřících jednotek (metrik), monitorovacích nástrojů, posouzení plnění cílů a efektivity procesů

Existuje několik různých strategií a přístupů pro dodávání služeb, které by měly být zváženy během fáze návrhu. Mezi nejznámější používané strategie patří insourcing, outsourcing, co-sourcing nebo Business Process Outsourcing (BPO). Rozdíl mezi prvními dvěma přístupy spočívá v tom, že insourcing spoléhá na využití interních organizačních zdrojů během všech aktivit v rámci poskytování služeb, zatímco outsourcing je založen na využívání prostředků externí organizace. V rámci outsourcingu je přenesena určitá vedlejší či podpůrná činnost podniku na jinou organizaci. Jeho výhodou může být snížení nákladů, možnost poskytovatele služeb zaměřit se na hlavní činnosti v zájmu jeho konkurenceschopnosti a svěření činnosti specializovanějším, proškolenějším a zkušenějším pracovníkům.

Kromě hlavních procesů tato fáze zahrnuje také další aktivity, jako je správa požadavků, správa dat a informací, a vývoj aplikací. V rámci vývoje aplikací se často uplatňuje specializovaný přístup Rapid Application Development (RAD), který se odlišuje od standardních vývojových metod, jako je například vodopádový model. Snahou přístupu RAD není získat všechny požadavky na počátku vývoje, jelikož požadavky se v průběhu vývoje mohou měnit. Je založen na inkrementálním a iterativním vývoji. Inkrementální vývoj znamená, že služba je vytvářena po částech. Jednotlivé části jsou vyvíjeny odděleně, prochází všemi fázemi vývojového cyklu a teprve po jejich spojení vznikne služba jako celek. Velkou výhodou tohoto přístupu je kratší doba doručení hotového řešení. Iterativní přístup je založen na

opakování vývojového cyklu služby a využití techniky prototypu pro lepší porozumění uživatelských požadavků a snazší provádění změn.

Výstupem fáze Service Design je tzv. Service Design Package (SDP). Ten je vytvářen pro každou novou službu, dále pro služby, na které jsou aplikovány větší změny, a rovněž pro služby, které budou vyřazeny z provozu. SDP je soubor dokumentů, které se zabývají všemi aspekty služby a specifikují příslušné požadavky pro všechny fáze jejího životního cyklu. V balíčku SDP například nalezneme popis celé potřebné infrastruktury (hardware, software, síťové prvky, data, aplikace, nástroje, dokumentace, technologie), procesů, procedur, metrik, apod. Vyskytuje se v něm také tzv. Service Programme, který reprezentuje všeobecný plán popisující všechny fáze služby a rozvrhující jednotlivé etapy vývoje služby. Součástí je i Service Transition Plan, což je plán popisující přechod služby do produkčního prostředí a zahrnující plány, politiky, technologie, nástroje, mechanismy a metody vytváření a testování služby. Mezi další prvky SDP můžeme zařadit například Service Operational Acceptance Plan a akceptační kritéria.

Procesy fáze Service Design:

- ☐ Service Level Management
- ☐ Service Catalogue Management
- ☐ Capacity Management
- ☐ Availability Management
- ☐ Information Security Management
- ☐ IT Service Continuity Management
- ☐ Supplier Management

Jednotlivé procesy z kapitoly Service Design jsou podrobně popsány v publikaci „Service Design“. [9]

3.2.1 Service Level Management

Service Level Management (SLM) je důležitým procesem každého poskytovatele IT služeb, jelikož je zodpovědný za stanovení a řízení úrovně poskytovaných služeb, která vychází z očekávání zákazníků. Proces se zabývá projednáváním, definováním, měřením a revidováním kvality IT služeb a umožňuje průběžné zlepšování kvality při akceptovatelných nákladech. SLM získává nezbytné informace o službě prostřednictvím portfolia služeb a je tudíž závislé na jeho kvalitním obsahu. Ve fázi návrhu služeb je SLM primárním rozhraním mezi zákazníkem a poskytovatelem, stejně jako je Service Desk ve fázi operativní.

3.2.1.1 Důležité pojmy

Service Level Agreement – SLA

SLA je písemným dokumentem, který reprezentuje dohodu mezi poskytovatelem IT služeb a zákazníkem, a popisuje klíčové cíle služby, priority, záruky a odpovědnosti. Tato smlouva specifikuje dostupnost, spolehlivost, podporu a další aspekty služby, které jsou významné pro zajištění požadované úrovně kvality.

☐ Smlouvy SLA založené na službách

Tento typ smlouvy specifikuje stejné podmínky dodávání služby pro všechny zákazníky. Tato dohoda je efektivním přístupem řízení úrovně služby v případě, že je poskytována stejná úroveň služeb ve všech oblastech byznysu. Příkladem takovéto služby může být email. Smlouvy založené na službě nejsou vhodné, pokud je nutno definovat specifické požadavky různých zákazníků.

☐ Smlouvy SLA založené na zákaznících

Dohoda založená na zákaznících je uzavírána s individuálním zákazníkem nebo zákaznickou skupinou, a týká se všech služeb, které příslušní zákazníci využívají. Tato smlouva může být například sjednána s finančním oddělením organizace ohledně všech služeb zajišťujících správu financí v organizaci, včetně účetního či výplatního systému. Tento přístup je často zákazníky preferován, jelikož všechny jejich požadavky na služby jsou definovány v jediném dokumentu.

☐ Víceúrovňové smlouvy SLA

Jedná se o poměrně složitější druh kontraktu. Jednotlivé smlouvy jsou strukturovány do několika úrovní – podniková úroveň, zákaznická úroveň a úroveň služeb. Takovéto rozložení SLA do více úrovní napomáhá snížit frekvencí pozměňování a pozdějších úprav ve smlouvách a rovněž napomáhá vyhnout se případným duplikátům.

Operational Level Agreement – OLA

OLA reprezentuje smlouvu poskytovatele IT služeb s určitou interní částí organizace, která se svou činností v různé míře podílí na podpoře poskytovaných služeb. Například se může jednat o skupinu zajišťující údržbu klimatizačního zařízení nebo oddělení síťové podpory, starající se o správu sítě. OLA zaručuje, že cíle definované v SLA nebudou v případě selhání podpůrných aktivit narušeny.

3.2.2 Service Catalogue Management

Jelikož IT infrastruktura organizací se neustále vyvíjí a je čím dál komplexnější, je nezbytné, aby existoval všeobecný přehled nad veškerými službami, které jsou organizací poskytovány. Tento přehled je zajištěn prostřednictvím již zmíněného portfolia služeb, jehož součástí je tzv. katalog služeb. V ITIL v2 byl koncept katalogu služeb zmíněn v rámci procesu Service Level Management, v nové verzi byl pro správu katalogu služeb vyhrazen nový proces.

Podstata tohoto procesu spočívá ve správě podrobných informací o službách, které jsou uloženy v katalogu služeb. Cílem je také zaručit přesnost a aktuálnost informací, a zachytit stav a vzájemné závislosti služeb. Katalog služeb zahrnuje všechny služby, které jsou již v provozu, a také služby, které jsou připravené k nasazení do živého prostředí. Kromě detailního popisu služeb katalog obsahuje rovněž informace o zákaznících a dodavatelích IT služeb. V mnoha organizacích je portfolio společně s katalogem služeb integrováno do systému CMS. Služby jsou obvykle v katalogu definovány jako samostatné konfigurační jednotky, což umožňuje jejich napojení na další entity správy služeb, jako jsou smlouvy SLA, incidenty, události, problémy. Změny v portfoliu služeb jsou prováděny procesem Change Management. Katalog služeb může být využit například procesem ITSCM v rámci analýzy dopadu na byznys (BIA) nebo procesem Capacity Management pro distribuci prostředků a pracovní zátěže.

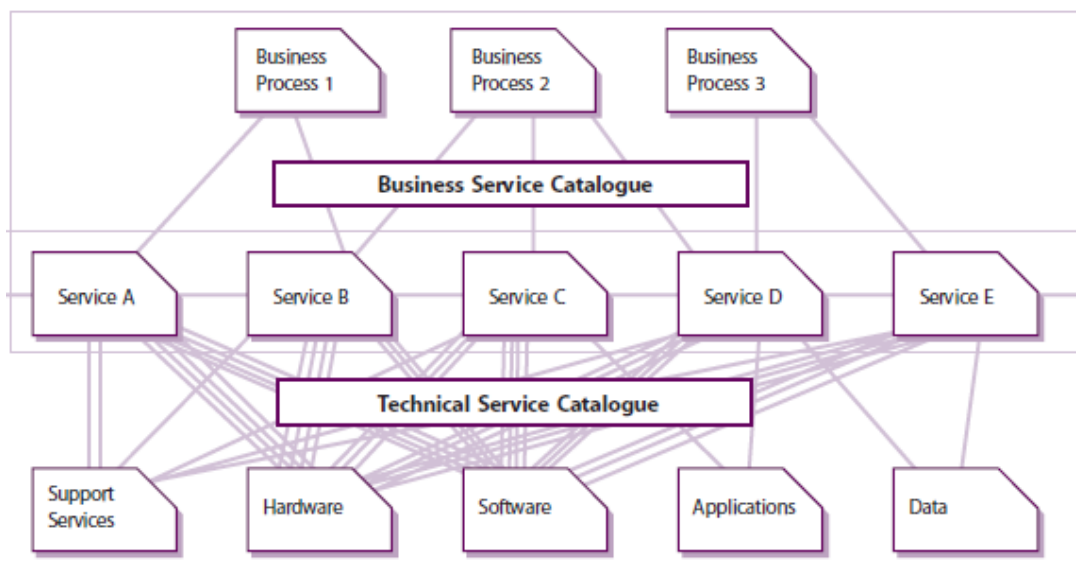
Katalog služeb je možno rozdělit na: byznys katalog a technický katalog (viz Obr. 5). Jejich kombinace poskytuje přehled nad tím, jaký dopad mohou způsobit incidenty či změny:

☐ Byznys katalog služeb

Tato část obsahuje detaily o všech službách poskytovaných zákazníkům a popisuje vztah služeb k daným oddělením organizace a procesům, které se o tyto služby opírají.

☐ Technický katalog služeb

Tento katalog je zaměřen na technickou stránku služeb, zachycuje souvislost služeb s jejich komponentami a podpůrnými službami, na kterých jsou závislé.



Obr. 5: Byznys katalog služeb a technický katalog služeb [9]

3.2.3 Capacity Management

Capacity Management je procesem, jehož cílem je včasné zajistit, že kapacita IT služeb a IT infrastruktury je schopna poskytnout úroveň kvality služeb, smlouvenou v procesu SLM, a definovanou ve smlouvách SLA a OLA. Capacity Management by měl udržovat rovnováhu mezi náklady a kapacitou tak, aby byly prostředky využity co nejefektivněji.

Jelikož obvykle dochází k častým změnám byznys požadavků, úkolem procesu je přizpůsobit těmto požadavkům a optimalizovat stávající prostředky, a zároveň efektivně odhadovat a plánovat prostředky potřebné k zajištění budoucí kapacity. Proces tedy zahrnuje reaktivní aktivity, přizpůsobující služby změnám (měření, monitoring) a proaktivní aktivity, které jsou založeny na vyvíjení vlastní iniciativy pro řízení kapacity služeb (předvídaní budoucích požadavků a trendů, plánování, rozpočtování, optimalizace služeb). Důležitým výstupem procesu je kapacitní plán (Capacity Plan), který je využíván všemi oblastmi byznysu a správy IT, a slouží jako základní prvek pro rozhodování.

Podpůrným nástrojem řízení kapacity je Capacity Management Information System (CMIS), tedy specializovaný informační systém obsahující všechny relevantní informace ohledně kapacity a výkonnosti služeb.

Řízení kapacity zahrnuje tři podprocesy a každý z nich využívá k vlastní analýze informace uložené v CMIS. Všechny podprocesy jsou tvořeny obdobnými aktivitami, liší se zejména svým zaměřením. Capacity Management obsahuje tyto podprocesy:

❑ Business Capacity Management

Hlavním záměrem prvního podprocesu řízení kapacity je správné posouzení a pochopení budoucích byznys požadavků na IT služby, a rovněž plánování a implementace dostatečné kapacity pro podporu nových či změněných služeb. Business Capacity Management se zabývá předvídaním, odhadem a analýzou trendů budoucích požadavků. Tyto požadavky plynou z fáze strategie služeb, konkrétně vycházejí z portfolia služeb, ve kterém se nachází podrobné informace o nových procesech, požadavcích na službu, změnách a o plánovaném zlepšování služeb.

❑ Service Capacity Management

Tento podproces se zaměřuje na řízení kapacity IT služeb, které jsou již nasazeny do živého operativního prostředí, a zodpovídá za kvalitu těchto služeb stanovenou prostřednictvím smluv SLA. Zahrnuje aktivity měření a monitorování, shromážděná data jsou následně zaznamenána a analyzována. Aktivity jsou prováděny pracovníky s bohatými technologickými znalostmi.

❑ Component Capacity Management

Cílem podprocesu Component Capacity Management je řízení a předvídaní výkonu, vytíženosti a kapacity samostatných IT komponent a technologií, které podporují IT služby – tj. infrastruktura, data, aplikace, aj. Tím je zaručeno optimální využití všech relevantních hardwarových a softwarových prostředků. Podproces se týká komponent, jako jsou například procesory, pevné disky, paměti, síťové prvky a další. Součástí komponent jsou obvykle monitorovací zařízení, která shromažďují a zaznamenávají nezbytná data. Tato činnost je zpravidla zajištěna a řízena fází Service Operation, která tak tomuto podprocesu poskytuje zpětnou vazbu.

3.2.4 Availability Management

Proces Availability Management se zaměřuje na záležitosti, které se týkají dostupnosti služeb a prostředků. Dostupnost je totiž jedním ze stěžejních měřítek kvality služby zákazníka. Cílem Availability Managementu je zaručit smlouvanou úroveň dostupnosti služeb. Správa dostupnosti zahrnuje reaktivní i proaktivní aktivity, je však nutno zmínit, že klíčovou aktivitou pro udržení požadované dostupnosti informačních technologií je měření a monitoring. Snahou tohoto procesu je průběžně provádět nákladově výhodnou optimalizaci a proaktivní vylepšování dostupnosti služeb a IT infrastruktury.

Stejně jako Capacity Management je i tento proces vyžadován ve všech fázích životního cyklu služby. Tím je zaručeno, že požadavky ohledně dostupnosti budou aplikovány na nové či změněné služby, a zároveň, že bude průběžně udržována vysoká stabilita a spolehlivost všech existujících služeb a souvisejících komponent.

3.2.4.1 Důležité pojmy

Dostupnost (Availability)

Dostupnost reprezentuje schopnost služby, komponenty nebo konfigurační jednotky poskytovat požadovanou funkčnost tehdy, kdy je to žádáno. Dostupnost je možno vypočítat na základě smlouvané doby fungování služby (Agreed Service Time - AST) a doby nečinnosti (downtime). Dostupnost se obvykle uvádí v procentech a lze ji vyjádřit dle následujícího vzorce:

$$Dostupnost (\%) = \frac{AST - downtime}{AST} * 100$$

Udržovatelnost (Maintainability)

Udržovatelnost je vyjádřena jednotkou, kterou nazýváme MTRS (Mean Time to Restore Service). Ta udává průměrný čas potřebný pro obnovu funkčnosti IT služby nebo konfigurační položky po selhání. Jednotka tedy vypovídá o tom, jak rychle může být služba obnovena. Doba nečinnosti služby zahrnuje všechny patřičné časové složky, které tvoří celkovou dobu nedostupnosti: doba detekce, doba vyšetřování, doba řešení, doba fyzických oprav a také doba znovuzavedení služby. Jednotka MTRS je závislá na mnoha faktorech, jako jsou MTRS jednotlivých komponent, dostupné zdroje, schopnosti zaměstnanců, politiky aj.

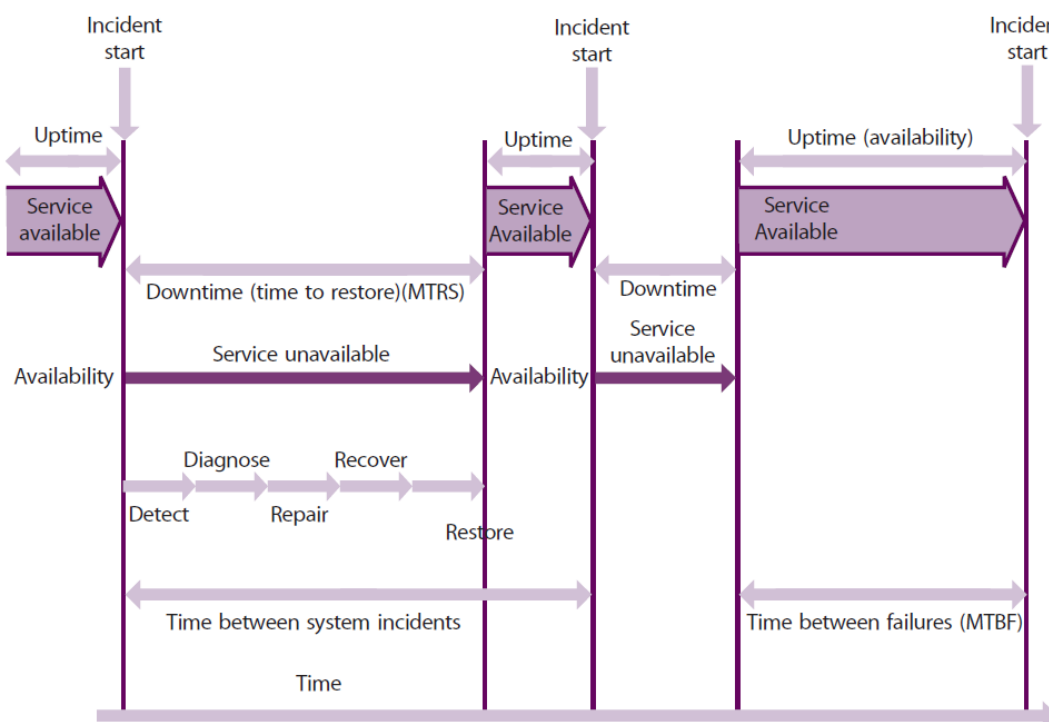
Spolehlivost (Reliability)

Spolehlivost je dalším zásadním faktorem dostupnosti služby, který je měřen jednotkou MTBF (Mean Time Between Failures). Jedná se o průměrnou dobu, po kterou je služba nebo konfigurační jednotka schopná fungovat dle smlouvaných funkčních požadavků.

Jiným ukazatelem spolehlivosti je metrika MTBSI (Mean Time Between Service Incidents), která udává průměrný čas mezi dvěma po sobě se vyskytujícími incidenty.

Provozuschopnost (Serviceability)

Provozuschopnost znamená schopnost dodavatele třetí strany dodržet smluvní podmínky kontraktu. V tomto kontraktu je obvykle specifikována smlouvaná úroveň dostupnosti, spolehlivosti a udržovatelnosti podpůrných služeb a komponent.



Obr. 6: Metriky dostupnosti služby v rámci životního cyklu incidentů [9]

3.2.4.2 Reaktivní aktivity a techniky

Měření a monitoring

Jedním z hlavních principů tohoto procesu je měření a vytváření zpráv o dostupnosti. Díky měření je možno srovnat skutečnou dostupnost služby se smlouvenou a průběžně ji optimalizovat a vylepšovat. Dostupnost je důležitým ukazatelem kvality služby a zákazníkem je vnímána jako velice důležitý faktor. Zákazníka obvykle zajímá frekvence a délka poruch, nebo jejich dopad.

Analýza selhání služby (Service Failure Analysis - SFA)

SFA je strukturovanou technikou zjišťování příčin poruch služeb. K odhalení důvodů nedostatečné dostupnosti služeb technika využívá velké množství různých datových zdrojů. Cílem SFA nejsou pouze vylepšení v oblasti technologií, ale rovněž vylepšení týkající se celé organizace, procesů, nástrojů a procedur. Mnoho aktivit, které probíhají v rámci této analýzy, úzce souvisí s operativním procesem Problem Management, a proto jsou v mnoha organizacích tyto aktivity prováděny jednotně.

3.2.4.3 Proaktivní aktivity a techniky

Existuje celá řada aktivit, které napomáhají proaktivně zvyšovat dostupnost IT služeb. Můžeme zde zařadit analýzy rizik, plánovanou a preventivní údržbu, používání paralelně fungujících duplikátních komponent (mirroring), průběžné revize a optimalizace. Dalšími příklady proaktivních technik správy dostupnosti jsou metody, jako například identifikace byznys kritických funkcí a procesů (Vital Business Functions – VBF), analýza řetězce chybových událostí (Fault Tree Analysis - FTA) nebo analýza dopadu selhání komponent (Component Failure Impact Analysis - CFIA). Podrobnosti o těchto metodách se nacházejí v oficiální publikaci „Service Design“. [9]

3.2.5 Information Security Management

Jelikož se neustále prohlubuje závislost každodenních byznys aktivit a komunikační infrastruktury na informačních technologiích, musí být v organizacích kladen čím dál větší důraz na bezpečnost veškerých informací. Informační bezpečnost by neměla být aplikována pouze na záležitosti technologické, nýbrž by měla být uvážena v širším kontextu, tedy v rámci celého byznysu. Měla by se týkat všech aspektů v oblasti správy IT služeb – tzn. technologií, procesů, personálu a partnerů.

V ITIL v3 již neexistuje samostatná publikace, zabývající se touto problematikou, jako tomu bylo u předchozí verze. Proces Information Security Management (ISM) je popsán v publikaci Service Design a jednotlivé záležitosti informační bezpečnosti jsou náležitě vysvětlovány v průběhu celého životního cyklu služby, tedy ve všech pěti publikacích.

Cílem správy informační bezpečnosti je chránit veškerá informační aktiva, tedy všechny informace, které jsou nezbytné pro chod společnosti a poskytování služeb, a jejichž narušení, nevyžádaná změna, odhalení, krádež či ztráta by mohly způsobit organizaci jisté škody. Aktiva jsou vystavena mnoha druhům hrozeb, které využívají jejich slabin, kterým říkáme zranitelnosti. Zranitelnosti mohou být různého charakteru, uveďme si nyní pár příkladů:

❑ Zranitelnosti technického charakteru

Příklady: Nespolehlivá dodávka elektrické energie, nedostatečný výkon a kapacita IT, nevhodné uskladnění záložních médií, absence bezpečnostních prvků zamezující přístup do místností s IT, nešifrovaná bezdrátová komunikace, atd.

❑ Zranitelnosti softwarového charakteru

Příklady: Neaktuální antivirová databáze, nepřítomnost antiviru a antispywaru, používání bezpečnostně slabých hesel, zastaralé operační systémy, používání neautorizovaného softwaru, nevhodně používaný internet, aj.

❑ Zranitelnosti organizačního charakteru

Příklady: Nedostatečné školení a důvěřivost zaměstnanců, absence monitorovacích aktivit, absence bezpečnostní politiky a směrnic, nedodržování pravidelných záloh, neomezený přístup k informacím, apod.

Vždy je třeba řádně zvážit, jak vysoký stupeň ochrany na danou informaci aplikovat, protože zpravidla platí, že čím vyšší stupeň bezpečnosti je vyžadován, tím vyšší budou náklady potřebné na příslušná opatření. Stanovit adekvátní úroveň ochrany je možné na základě detailní analýzy rizik.

Úspěšnost správy informační bezpečnosti tkví v pečlivé ochraně informací před narušením jejich důvěrnosti, dostupnosti, integrity a autentičnosti, a to během jejich celého životního cyklu.

❑ Důvěrnost

Zajištěním důvěrnosti zabezpečíme, že k daným informacím mají přístup pouze autorizované osoby a systémy. Příkladem narušení důvěrnosti může být čtení cizího emailu.

❑ Dostupnost

Dostupností rozumíme, že daná informace je k dispozici autorizovaným osobám a systémům právě v době, kdy je přístup povolen. Příkladem narušením dostupnosti může být selhání při spuštění služby z důvodu neúmyslného smazání datového souboru.

❑ Integrita

Integrita informací spočívá v přesnosti a kompletnosti informací, a může být porušena neautorizovanými systémy, procesy či osobami, které příslušná data neoprávněně modifikují. Typickým příkladem narušení informační integrity je modifikace dat uložených na pracovním počítači, která byla provedena počítačovým virem.

❑ Autentičnost

Zajištění autentičnosti staví na ujištění, že veškeré obchodní styky, transakce a kontrakty jsou autentické a nefalšované, a že identita osob a systémů přistupujících k informacím je předem známá a ověřená. Příkladem neautentického přístupu je tzv. krádež identity, kdy se určitá osoba vydává za jinou za účelem zisku citlivých informací organizace, apod.

3.2.5.1 Aktivita a techniky

Klíčovými aktivitami, které se podílí na správě informační bezpečnosti, jsou: zavedení a revize politik informační bezpečnosti a podpůrných politik, jejich prosazování v organizaci, posouzení a klasifikace všech informačních aktiv, řízení bezpečnosti a posuzování rizik, monitorování a správa bezpečnostních incidentů, analýza a eliminace dopadů bezpečnostních útoků a incidentů na byznys, bezpečnostní audity, aj.

Použité metody, nástroje a techniky v rámci aktivit správy informační bezpečnosti by měly naplňovat bezpečnostní strategii. Za jejich vhodné použití je zodpovědný tzv. information security manager (manažer informační bezpečnosti). Je zřejmé, že informační bezpečnost je neustále probíhající proces, který musí být průběžně řízen. Informační bezpečnost musí být integrovanou součástí každé služby a každého systému.

3.2.6 IT Service Continuity Management

V dnešní době musí podniky čelit nespočetnému množství rizik z důvodu výskytu různorodých přírodních katastrof a technických poruch. V důsledku toho může dojít k narušení byznysu a tím i výraznému poklesu výkonnosti služby, popř. dojde k jejímu absolutnímu výpadku.

Prioritou procesu IT Service Continuity Management (ITSCM) je omezit dopady na IT služby, které mohou být následkem takovýchto incidentů, a chránit kontinuitu byznys procesů v organizaci. K tomuto účelu proces využívá dobře známé metody, jako je analýza dopadu (Business Impact Analysis - BIA), která kvantitativně určuje míru dopadu selhání služby na byznys, a analýza rizik (Risk Analysis - RA), která se zabývá identifikací potenciálních hrozeb a posouzením rizik v rámci kontinuity služeb. Odpovědností procesu je také vytvářet tzv. plány kontinuity a plány zotavení. ITSCM je součástí širšího podnikového procesu, který se nazývá Business Continuity Planning (BCP).

3.2.7 Supplier Management

Hlavním cílem Supplier Managementu je správa dodavatelů a služeb, které jsou organizaci těmito dodavateli poskytovány. Dodavatelé jsou považováni za třetí stranu v rámci poskytování IT služeb a jejich úkolem je dodávat produkty nebo poskytovat podpůrné služby, které jsou potřebné pro provoz IT služeb. Smyslem procesu je získat výměnou za finanční prostředky určitou přidanou hodnotu od dodavatele pro poskytované IT služby a zajistit, že dodavatelé důsledně plní cíle ustanovené v příslušných smlouvách.

Všechny aktivity procesu musí vycházet ze strategie a politik dodavatele. Pro zajištění konzistence a efektivity implementace politik se obvykle vytváří tzv. databáze dodavatelů a kontraktů (Supplier and Contract Database - SCD), která bývá integrovanou součástí CMS nebo SKMS. Databáze obsahuje všechny náležité informace o dodavatelích a smlouvách, o typu služeb nebo produktů, a jejich souvislosti s ostatními konfiguračními jednotkami.

Je důležité, aby byly precizně definovány a externím dodavatelem formálně schváleny všechny náležitosti kontraktu. Ve smlouvě by měly být specifikovány patřičné odpovědnosti a cíle dodavatele. Kontrakty pak musí být spravovány organizací během celého životního cyklu. Supplier Management zahrnuje implementaci politik dodavatele, správu SCD, klasifikaci dodavatelů, posouzení rizik, jednání a revizi kontraktů, řízení výkonnosti dodavatelů, aj.

3.3 Service Transition

Cílem fáze Service Transition je převést požadované služby do provozního prostředí. Tato fáze přijímá výstupy z předchozí fáze Service Design a následující operativní fázi předává všechny elementy potřebné pro provoz a údržbu služeb. Service Transition je rovněž zodpovědná za zajištění veškerých úprav a změn ohledně služby, které během provozu nastanou. Zaměřuje se na implementaci služby z různých pohledů, nezabývá se pouze prostým zavedením služby a jejím použitím v normálních podmínkách. Musí být zajištěno, že služba bude fungovat i za dlouhodobých abnormálních nebo extrémních podmínek. [10]

Souhrn cílů Service Transition:

- ☐ Plánovat a řídit schopnosti a zdroje za účelem vytváření, testování a distribuce releasů do produkčního prostředí a zřídit službu dle požadavků zákazníka a ostatních zainteresovaných osob
- ☐ Zajistit integritu všech identifikovaných konfiguračních položek (aktiv)
- ☐ Poskytnout kvalitní řízení znalostí a informací zejména pro procesy Change a Release and Deployment Management
- ☐ Poskytnout efektivní opakovatelný mechanismus pro vytváření, instalaci a nasazování releasů do testovacího a produkčního prostředí
- ☐ Zajistit účinné řízení změn včetně posouzení jejich možných rizik a přínosů

Procesy fáze Service Transition:

- ☐ Transition Planning and Support
- ☐ Service Asset and Configuration Management
- ☐ Change Management
- ☐ Release and Deployment Management
- ☐ Service Validation and Testing
- ☐ Knowledge Management
- ☐ Evaluation

Jednotlivé procesy z kapitoly Service Transition jsou podrobně popsány v publikaci „Service Transition“. [11]

3.3.1 Transition Planning and Support

Transition Planning and Support je jedním z nových procesů ITIL v3. Tento proces byl v minulé verzi rámce částečně zakomponován do procesu Release Management, v třetí verzi vystupuje proces odděleně a přináší s sebou výrazná vylepšení. Protože podstatou tohoto procesu je řízení projektů v rámci fáze Service Transition, zabývá se tato část publikace různými aspekty Project Managementu – tedy disciplínou, pojednávající právě o řízení projektů. ITIL v3 však nezkoumá projektové řízení dopodrobna, spíše zdůrazňuje jeho nejdůležitější aktivity a propojení s ostatními procesy ITSM.

Cílem procesu Transition Planning and Support je plánování a koordinace všech zdrojů potřebných ve fázi Service Transition tak, aby byly naplněny požadavky specifikované ve fázi Service Design, konkrétně v SDP. Proces zajišťuje řízené plánování změn, dodržování zavedených standardů, koordinaci kompetentních osob, týmů a dalších prostředků. Rovněž jsou identifikována a omezována rizika, která by mohla narušit provoz služeb. Hlavním přínosem procesu pro byznys je, že umožňuje poskytovateli vypořádat se s velkým množstvím změn a releasů.

3.3.1.1 Aktivita a techniky

Stanovení strategie přechodu

Nejprve je specifikován obecný přístup k organizaci přechodu služby a alokaci zdrojů. V rámci strategie jsou identifikovány a popsány cíle, rozsah, standardy, smlouvy, všechny zainteresované osoby a zodpovědnosti, kritéria úspěchu, plány pro řízení změn, správu aktiv, konfiguraci a znalostí, a další.

Příprava fáze Service Transition

Během přípravy jsou revidovány a odsouhlaseny všechny potřebné vstupy z ostatních fází cyklu služby, jako SDP, akceptační kritéria služby, apod. Aktivita také zahrnuje časové rozvržení požadavků na změnu (RFCs) a ověřuje, zda jsou před zahájením fáze přechodu služby řádně zaznamenány základní linie konfigurací (baselines).

Plánování a koordinace Service Transition

Plánování a koordinace specifikuje aktivity pro uvolňování a nasazování releasu do testovacího a produkčního prostředí. Aktivita se zabývá alokací zdrojů, rozpočtováním, plánováním důležitých milníků a termínů doručení služby, pracovním prostředím, infrastrukturou, apod.

Následně jsou revidovány všechny patřičné plány a dojde k zhodnocení několika důležitých faktorů. Například se posoudí, zda byla zvážena všechna rizika způsobující negativní dopad na organizaci, technologie a náklady, a ověří se kompatibilita nových konfiguračních položek s konfiguračními položkami cílového prostředí.

Podpora

Záměrem této aktivity je poskytnout rady a podporu všem zainteresovaným stranám. Tým pro plánování a podporu napomáhají všem zainteresovaným osobám proniknout do podstaty plánovaného přechodu a porozumět náležitým procesům a podpůrným nástrojům. Protože jsou aktivity fáze Service Transition monitorovány, může být jejich průběh snadno srovnáván s jednotlivými plány.

3.3.2 Service Asset and Configuration Management

Proces SACM je podpůrným procesem byznysu a ostatních procesů. Účelem procesu je spravovat všechna aktiva, která formují organizační infrastrukturu, identifikovat konfigurační položky, nést za ně odpovědnost a zajistit jejich integritu napříč celým životním cyklem služby. SACM poskytuje organizaci věrohodné informace o jednotlivých prvcích infrastruktury – jako jsou hardware, software, dokumentace, lidé, lokality, komunikační prvky a udržuje přehled o vztazích mezi nimi. Pro správu rozsáhlé a složité infrastruktury využívá SACM podpůrný systém, zvaný Configuration Management System (CMS), který spolupracuje s CMDB obsahující aktuální data o všech prvcích ICT infrastruktury.

3.3.2.1 Důležité pojmy

Service Assets (Aktiva služby)

Jedná se o schopnosti či prostředky, které jsou organizací využívány při poskytování služeb. Prostředky mohou zahrnovat finance, infrastrukturu, aplikace či informace. Schopnosti napomáhají organizaci vyvíjet a řídit zdroje za účelem vytvoření přidané hodnoty služeb. Schopnosti jsou typicky založené na zkušenostech a znalostech, a proto jsou spojeny s procesy, technologiemi, systémy a lidmi v podniku. Aktiva můžeme podrobněji rozdělit na procesní (metody, algoritmy, procedury), informační (zákazníci, kontrakty, služby, události, projekty), aplikační (software, hardware, dokumenty, skripty, instrukce), infrastrukturní (počítače, aplikace, síťové prvky, úložné systémy, monitorovací systémy, komunikační prvky), a další.

Configuration Items – CI (Konfigurační položky)

Konfiguračními položkami rozumíme aktiva – tedy prostředky mající pro organizaci určitou hodnotu, komponenty služby či další položky, které jsou pod správou SACM. Konfigurační položky jsou vybírány dle stanovených kritérií. Jsou klasifikovány a identifikovány tak, aby byly zpětně výsledovatelné v rámci životního cyklu služby. Mohou se lišit typem, složitostí i rozsahem. CI může tvořit například celá služba, která se skládá z hardwarových komponent, softwaru, popř. i dokumentace. Naproti tomu se může jednat pouze o primitivní konfigurační položku, jako je jednoduchý modul programu nebo prvek v síti.

Configuration Baseline (Konfigurační základní linie)

Tzv. konfigurační baseline zachycuje stav konfigurační položky v určitém momentě (snapshot). Baseline popisuje strukturu a veškeré detaily dané konfigurace, a slouží jako základ pro další aktivity. Základní linie je považována za původní stav položky a tím umožňuje porovnání původního stavu položky s jejím současným stavem.

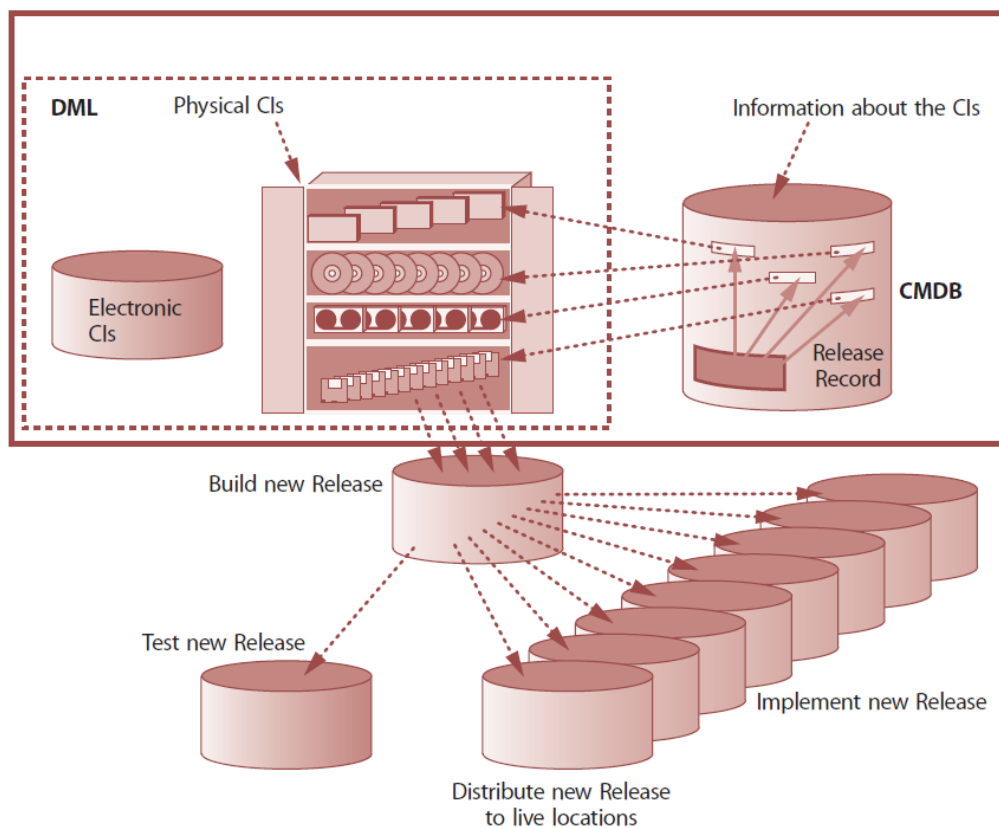
Configuration Management Database – CMDB

CMDB obsahuje patřičné údaje o konfiguračních položkách, jejich verzích, cenách, licencích a udržuje historii položek pro zpětnou sledovatelnost. CMDB rovněž zachycuje vztahy a souvislosti mezi jednotlivými komponentami služby, ukládá informace o incidentech, problémech, známých chybách, změnách a releasech. Součástí obvykle jsou i podnikové informace o zaměstnancích, dodavatelích, byznys útvarech atd.

The Definitive Media Library – DML

DML je zabezpečená knihovna, která obsahuje kopie konečných a autorizovaných verzí všech softwarových a dokumentových konfiguračních položek, popř. licencí a softwarových

klíčů. Všechny položky musí předem projít kontrolou ověření kvality. Položky mohou být uloženy v elektronické či fyzické podobě a informace o nich jsou zaznamenány v CMDB (viz Obr. 7). Uložený software je spravován Change Managementem a Release and Deployment Managementem.



Obr. 7: Souvislost The Definite Media Library s CMDB [11]

Definitive spares

Definitive spares je fyzickým úložištěm všech záložních komponent a systémů IT infrastruktury. Podrobné informace o těchto konfiguračních jednotkách jsou zaznamenány v CMDB a za jejich správu a nasazování do provozu odpovídá proces Release and Deployment Management. Záložní komponenty jsou využívány například tehdy, když selže určitá komponenta, která je součástí ostrého provozu služeb, a umožní tak rychlé zotavení služby z vyvolaného incidentu.

3.3.2.2 Aktivita a techniky

Identifikace konfiguračních položek

Podstatou identifikace je definovat kritéria pro výběr konfiguračních položek a komponent, z kterých se skládají, vybrat konfigurační položky podle stanovených kritérií a specifikovat relevantní atributy jednotlivých položek. Každá individuální položka je unikátně identifikovatelná dle identifikátoru a čísla verze. Dále se zaznamenávají informace o vztahu k ostatním položkám v rámci hierarchického uspořádání, informace o souvisejících dokumentech, umístění a vlastníkově položky, aj.

Správa konfigurací

Správa konfigurací zahrnuje registraci nových konfiguračních jednotek a jejich verzí, dále změny konfiguračních jednotek týkající se jejich stavu, atributů, rolí, vlastnických práv, licencí apod. V rámci správy konfigurací se vykonává periodická kontrola a porovnání fyzických položek v organizaci s údaji v CMDB a aktualizace této databáze v případě změn či nepřesností.

Zpráva o stavu konfigurace

Tato aktivita spočívá ve vytvoření a zaznamenání zprávy popisující konfigurační položky a jejich stav. Každá konfigurační položka se totiž nachází v určitém stavu (schválená, ve vývoji, instalována, aj.). Vytvořená zpráva popisuje současný stav položek, poslední verze softwarových položek a jejich stav, historii změn, přehled otevřených problémů, RFC apod. Tato zpráva rovněž zahrnuje oznámení o neautorizovaném použití hardwaru či softwaru.

Verifikace a audit

Cílem verifikačních revizí a auditu v rámci Configuration Managementu je zajistit soulad mezi dokumentovanými základními liniemi (baselines) a skutečným prostředím byznysu, ke kterému se vztahují, a ověřovat fyzickou existenci konfiguračních položek v organizaci nebo v DML. Součástí této aktivity je také ověření, zda je před vydáním každého releasu vytvořena konfigurační dokumentace.

3.3.3 Change Management

Záměrem procesu Change Management je zajistit, že všechny změny týkající se poskytovaných služeb jsou zaváděny řízeným způsobem, precizně plánovány, testovány, implementovány, dokumentovány a vyhodnocovány.

Změnou rozumíme přidání, úpravu nebo odstranění plánované a autorizované služby nebo její komponenty včetně dokumentace. Potřeba změny může vzniknout jako následek problému z procesu Problem Management, mnoho změn ovšem vychází z proaktivního hledání přínosů pro byznys, jako je snižování nákladů nebo vylepšování služby. Je důležité, aby všechny změny byly udržovány v CMDB a aby byly používány standardizované metody a procedury změn. V rámci plánování změn je nutné zvážit možná rizika pro byznys. [10]

3.3.3.1 Důležité pojmy

Change Advisory Board - CAB

Change Advisory Board je seskupení lidí, které se zabývá schvalováním změn a napomáhá Change Managementu hodnotit změny, stanovovat jejich prioritu a rizika. Členové CAB musí rozumět potřebám zákazníků a uživatelů, stejně jako technickému záležitostem a podpůrným funkcím. CAB obvykle zahrnuje manažera změn, zákazníky, zástupce uživatelských skupin, aplikační vývojáře, technické experty, zaměstnance podpory služeb, popř. dodavatele.

Change Schedule - CS

Change Schedule je důležitým dokumentem procesu Change Management, ve kterém je uveden časový plán implementace všech schválených změn. Termíny jednotlivých změn musí být odsouhlaseny příslušnými zákazníky, Service Deskem a Service Level Managementem. Někdy je tento dokument také nazýván pojmem Forward Schedule of Change.

Request for Change – RFC

Celý proces správy změn je nastartován vznikem požadavku na změnu, tzv. Request for Change. RFC obsahuje všechny podstatné informace potřebné pro změnu: popis ovlivněných konfiguračních jednotek, důvod ke změně, důsledek neprovedení změny, priorita, dopad změny na byznys, reference na implementační plán atd. Možné důvody pro vytvoření RFC:

- ☐ Požadavek k vyřešení incidentu nebo problému
- ☐ Zavedení nové CI nebo odstranění CI
- ☐ Provedení upgradu komponenty v IT infrastruktuře
- ☐ Změna byznys požadavků
- ☐ Nová nebo změněná legislativa
- ☐ Změna umístění
- ☐ Nespokojenost zákazníka

3.3.3.2 Modely změn

Model standardní změny (Standard Change Model)

Tento model se využívá pro předem schválené, opakující se, dobře otestované změny, které se vyznačují svým nízkým rizikem. Většinou je aplikován na operativní změny týkající se údržby služby. Pro implementaci standardní změny není nutné vytvářet RFC. Jednotlivé aktivity jsou řízeny různými mechanismy a modely, které zahrnují dobře známé, dokumentované a osvědčené úkoly. Většinou je standardní změna prováděna jako Service Request, tedy prostřednictvím procesu Request Fulfilment. Příkladem standardní změny je upgrade PC nebo jeho přemístění, požadavek na obnovení hesla nebo změnu přístupových práv uživatele k službě.

Model naléhavé změny (Emergency Change Model)

Tento model je používán pouze pro velmi kritické změny. Umožňuje rychlé zotavení služby z rozsáhlého selhání a obnovení její dostupnosti. Model je možno také aplikovat na preventivní změny před bezprostředně hroící poruchou služby (např. implementace bezpečnostní záplaty). Využití tohoto modelu by mělo být minimální, jelikož tento typ změny je náchylnější k chybám. Naléhavé změny vyžadují velkou pozornost a rychlé zpracování, a proto je vhodné stanovit specifické procedury, které umožní jejich rychlé zavedení.

Model normální změny (Normal Change Model)

Normální model je kompletní model změn, které musí před implementací projít všemi fázemi procesu Change Management – posouzením, autorizací i schválením orgánem CAB.

3.3.3.3 Aktivita a techniky modelu normální změny

Vytvoření a záznam RFC

Změna může být vyvolána jednotlivcem nebo organizační skupinou, která změnu požaduje. Nejprve dojde k vytvoření a záznamu tzv. RFC z několika možných důvodů, které byly již zmíněny. Při postupu RFC jeho životním cyklem dochází k průběžné aktualizaci všech souvisejících záznamů, dokumentů a konfiguračních jednotek v databázi CMDB. Rovněž jsou zaznamenány odhadované a skutečné zdroje, náklady a výsledek změny.

Revize RFC

Po zaznamenání RFC nastává aktivita, která přezkoumává jednotlivé záznamy a odfiltruje ty požadavky, které jsou neproveditelné, požadavky s neúplným popisem a v neposlední řadě také opakující se duplikátní požadavky.

Posouzení a zhodnocení RFC

Je důležité zvážit všechna rizika změny a možný dopad na aktiva, konfigurační jednotky a samotnou službu. Kromě dopadu a rizik je každá změna ohodnocena dalšími faktory - cenou, naléhavostí a přínosy. Na základě dopadu a naléhavosti je pak změně přiřazena priorita. Po zhodnocení RFC a stanovení priorit dochází k plánování a časovému rozvržení změn.

Schválení změny

Každou změnu je potřeba formálně schválit. Schválení může provést oprávněná osoba, skupina lidí nebo osoby s určitou rolí. Jelikož se změny liší typem, velikostí a rizikem, zavádí se obvykle několik autorizačních úrovní, které jsou reprezentovány různými autoritami (např. CAB, správní rada, aj.).

Koordinace implementace změny

V momentě, kdy byl daný požadavek autorizován, může být předán příslušným technickým odborníkům, kteří změnu aplikují v reálném prostředí. Samotná realizace změn spadá zejména pod proces Release and Deployment Management. Přesto hraje Change Management významnou roli při implementaci změny, jelikož ji koordinuje a zajišťuje, že implementace proběhne tak, jak byla časově naplánována. Proces správy změn dohlíží také nad tím, aby všechny uskutečněné změny byly řádně otestovány.

Revize a uzavření záznamu o změně

Na závěr je zaznamenán výsledek změny a záznam o změně je uzavřen, spolu se souvisejícími incidenty, problémy či známými chybami. Po určité stanovené době musí být změna přezkoumána (Post Implementation Review – PIR), aby se zjistilo, zda byl úspěšně naplněn její záměr, zda jsou zákazníci se změnou spokojeni, zda nebyly překročeny plánované náklady atd.

3.3.4 Release and Deployment Management

Dalším důležitým procesem z řady procesů fáze Service Transition je Release and Deployment Management. Jeho cílem je sestavit službu, zavést ji do produkčního prostředí a umožnit efektivní využití nové či změněné služby, vyhovující požadavkům všech zainteresovaných osob. Proces zahrnuje aktivity vytváření, testování a nasazování služeb, které byly předem specifikovány v Service Design. Výhodou procesu pro poskytovatele je, že je schopen dodávat změny ve službách mnohem rychleji s menším úsilím, nižšími vynaloženými náklady a minimálním rizikem. Dalším velkým přínosem pro organizaci i pro zákazníka je snížení negativních dopadů na poskytované služby – minimalizace incidentů.

Výsledkem procesu je tedy zavedení kvalitní a konzistentní změny do IT infrastruktury, která je řádně otestovaná, akceptovaná ze strany zákazníka a náležitě zaznamenaná pro případnou potřebu dalších procesů správy IT služeb.

3.3.4.1 Důležité pojmy

Release

Release je soubor nových nebo změněných konfiguračních položek, potřebných pro implementaci schválených změn do produkčního prostředí. Konfigurační položky mohou zahrnovat software, hardware, dokumentace aj. Release obvykle zahrnuje určité množství oprav a vylepšení služeb.

Releasy je možno rozdělit do tří kategorií v závislosti na množství nové funkcionality či rozsahu změn:

❑ Major releases (Hlavní releasy)

Tyto releasy obvykle zahrnují velké množství nové funkcionality a často se týkají komplexnějších komponent – hardware, software. Hlavní release či upgrade nahrazuje všechny předchozí vedlejší releasy a naléhavé opravy.

❑ Minor releases (Vedlejší releasy)

Minor releasy obsahují menší opravy a vylepšení služeb zpravidla související s menším počtem komponent, většinou opravují známé chyby. Nahrazují všechny naléhavé opravy.

❑ Emergency fixes (Naléhavé opravy)

Naléhavé opravy obvykle eliminují malé množství známých chyb, které se vyskytly v IT infrastruktuře v souvislosti s poskytováním služeb a mohou být rychle opraveny.

Release unit

Release unit popisuje část služby či IT infrastruktury, která je obvykle uvolňována jako celek na základě release politik (Release Policy). Tyto jednotky se mohou lišit v závislosti na typu a položkách komponent služby, jako je hardware nebo software. Cílem Release Managementu je stanovit příslušnou úroveň release jednotky pro každou část služby. Například release jednotkou pro byznys kritické aplikace by měla být celá aplikace, aby mohla být aplikace otestována komplexně. V jiných případech se může jednat pouze o moduly aplikací či další části hierarchického uspořádání komponent služby.

Release Package

Individuální releasy mohou být seskupovány do balíčků (Release Package). Seskupení releasů do balíčků je vhodné například tehdy, pokud změny určité komponenty vyžadují současnou implementaci změn dalších komponent či systémů. Tyto balíčky mohou snížit pravděpodobnost používání starého nebo nekompatibilního softwaru. Release Package může být tvořen jedinou release jednotkou nebo strukturou více release jednotek.

3.3.4.2 Způsoby uvolňování a nasazování releasů

Big bang (Velký třesk) vs. Phased (Postupný)

Metoda „Velkého třesku“ je založena na tom, že nová nebo změněná služba je zavedena v jednom kroku do všech lokalit a ke všem uživatelům.

„Postupnou“ metodou se služba nasazuje nejprve pro určitou uživatelskou základnu, v dalších krocích se operace opakuje pro další uživatele. Lze využít různých variací postupného

nasazování. Například mohou být služby nasazovány postupně dle geografických oblastí. Další alternativou je metoda, pomocí které jsou postupně v několika fázích zaváděny různé typy elementů služeb (např. nejdříve hardware, pak software a následně je provedeno školení uživatelů).

Push vs. Pull

Přístup „push“ spočívá v tom, že nová nebo změněná komponenta je nasazována z centrálního místa a je jakoby vytlačována do cílových míst. To znamená, že aktualizovaná služba je doručena všem uživatelům. Uživatel si tedy nemůže sám vybrat dobu pro aktualizaci. Při využití tohoto přístupu musí být dostupná příslušná data na všech uživatelských stanicích.

U přístupu „pull“ je software umístěn do centrálního úložiště a uživatelé mají možnost stáhnout si aktualizaci přes internet a to v momentě, kdy chtějí. V případě, že si uživatel nestáhne nový release do určité doby, je obvykle přinucen aktualizaci přijmout přístupem „push“.

3.3.4.3 Aktivita a techniky

Plánování a příprava tvorby, testování a nasazování releasů

V rámci aktivity plánování jsou vytvořeny release plány a plány nasazení, které formují část obecného plánu Service Transition a definují modely použité pro tvorbu a testování služby. Často využívaným modelem je tzv. V-model, který může být kombinován s dalšími přístupy vývoje služby, jako je např. vodopádový model, nebo využívá praktiky iterativních modelů - prototypový model, model RAD, aj. V-model je popsán v kapitole Service Validation and Testing.

Plány dokumentují rozsah a obsah releasu, ovlivněné osoby, odpovědné týmy, komunikační strategii, zabývají se posouzením možných rizik. Mohou se lišit v závislosti na velikosti a složitosti prostředí a množství změněných nebo nových služeb. Součástí jsou také plány doručování služeb, logistické plány, finanční plány a plány tzv. pilotních releasů (pilots). Pilotní releasy slouží k prvotnímu testování životaschopnosti nové nebo změněné služby v rámci malé části uživatelské základny.

Před tím, než dojde ke schválení fáze tvorby a testování releasu, musí být návrh služby validován. Validací rozumíme porovnání návrhu se specifikací nové či změněné služby.

Tvorba a testování

Aktivita zahrnuje pořízení, zakoupení a testování konfiguračních jednotek a komponent releasů, sestavování a integraci komponent, kompilaci releasů do balíčků, správu prostředí pro vytváření a testování releasů. Také se zabývá správou konfigurací, tzn. správou verzí, bezpečnostních procedur a nastavováním přístupových práv. Během tvorby a testování releasů je vhodné využívat opakovatelné praktiky a znovupoužitelné komponenty.

Testování služby

Testovací aktivity jsou koordinovány test managementem, jehož úkolem je plánovat a řídit provádění testů. Tímto se podrobně zabývá proces Service Validation and Testing.

Jedním ze stěžejních přístupů testování je použití již zmíněných pilotních releasů. Ty mohou odhalit části služby, které plně nevyhovují požadavkům a vyžadují další zdokonalování, popř. změny v návrhu.

Plánování a příprava nasazení

Během těchto aktivit je organizace připravována na nasazení releasu. Je vytvářen plán nasazení, který přiřazuje jednotlivým aktivitám v rámci nasazování releasu (např. školení uživatelů) potřebné prostředky, tedy především kompetentní osoby či skupiny osob. Plán musí být odsouhlasen všemi zainteresovanými osobami – tj. zákazníky, uživateli, provozem a podporou uživatelů.

Nasazení releasu

V momentě, kdy jsou plány schváleny, může začít samotné nasazování služby. Nasazení spočívá v distribuci a instalaci služby a všech souvisejících komponent – tj. podpůrných služeb, aplikací, prvků infrastruktury a dalších zařízení. Proběhne také náležitá konfigurace služeb a jsou zavedena všechna nezbytná data. Rovněž je publikována a distribuována veškerá dokumentace, kterou budou uživatelé potřebovat k využívání služby a dojde k aktualizaci databáze Service Catalogue. Pro úspěšné nasazení a správu nové či změněné služby je žádoucí mobilizovat všechny kompetentní osoby s adekvátními dovednostmi.

Kromě nasazování releasu pokrývá tato aktivita i vyřazování nepotřebných služeb či komponent z produkčního prostředí. Opomenutí této činnosti by mohlo vést například ke zbytečnému zatížení kapacity, pozdějšímu používání nepodporovaného softwaru či porušení licencí.

Verifikace nasazení releasu

Jakmile je dokončena fáze nasazování releasu, je důležité ověřit, zda jsou všechny zainteresované strany, tedy především její uživatelé, schopny službu používat. K ověřování se využívají zejména tzv. průzkumy spokojenosti (satisfaction surveys).

Počáteční podpora služby (Early Life Support - ELS)

Úspěšná verifikace aktivuje tzv. počáteční podporu služby, která zajišťuje přechod služby do operativní fáze, sleduje některé kvalitativní atributy služby – především její výkon a stabilitu, a v případě, že služba nevyhovuje daným kritériím, může být vylepšována dle procesů fáze Continual Service Improvement. Ve fázi ELS mohou být případné problémy se službou vyřešeny poměrně rychle a uživatel tak nemusí čelit výpadkům služby.

Závěrečná revize a uzavření

Na závěr procesu je poskytnuta finální zpětná vazba od zákazníka. Zjistí se, zda jsou uživatelé se službou spokojeni, zda byl proveden adekvátní transfer znalostí, zda byli uživatelé dostatečně vyškoleni. Všechny opravy a změny týkající se služby jsou dokončeny, problémy, známé chyby a jejich řešení jsou náležitě dokumentovány. Služba je nyní připravena pro přechod z fáze ELS do fáze produkční.

3.3.5 Service Validation and Testing

Testování je jednou z nejdůležitějších disciplín pro zajištění kvality služeb a výrazně se podílí na zajištění přidané hodnoty byznysu zákazníka. Service Validation and Testing ověřuje kvalitu služeb během celého životního cyklu, hlavní využití však spočívá v podpoře procesu Release and Deployment Management. Proces testuje užitečnosti (utilities) a záruky (warranties) služby, které byly stanoveny v Service Design – tj. funkcionalita, dostupnost, kontinuita, bezpečnost, použitelnost, apod.

Testování je velmi důležitou součástí vývoje služby. Přesto bývá často opomíjeno nebo na tuto fázi není kladen patřičný důraz, především kvůli nedostatku financí. Neadekvátní testování může zapříčinit množství problémů: větší počet chyb a s tím související časté selhávání služeb, přibývající incidenty, větší zátěž na Service Desk a odborníky pro podporu, ztráta dobré pověsti organizace, zvýšení nákladů nebo vytvoření služby s nesprávnou funkcionalitou a malým potenciálem použití. Potřeba důkladného testování neustále roste, velký důraz na prvotřídní kvalitu a spolehlivost IT služeb je kladen v mnoha oblastech, zejména v lékařství nebo v automobilovém a leteckém průmyslu.

3.3.5.1 Verifikace a validace

Testování je obecně založeno na dvou přístupech, kterými jsou verifikace a validace. Zatímco verifikací ověřujeme, zda výsledná služba vyhovuje specifikaci a podmínkám stanoveným na počátku jejího vývojového cyklu, validací můžeme potvrdit, že specifikovaná funkcionalita odpovídá skutečným požadavkům a cílům zákazníka. Validace požadavků je zahájena již v okamžiku, kdy jsou požadavky definovány. Verifikace nám tedy dává odpověď na otázku, zda je služba vytvářena správně, a validací se ujistíme, zda je vytvářena správná služba, tzn. služba, která naplňuje očekávání klientů.

3.3.5.2 Typy testů

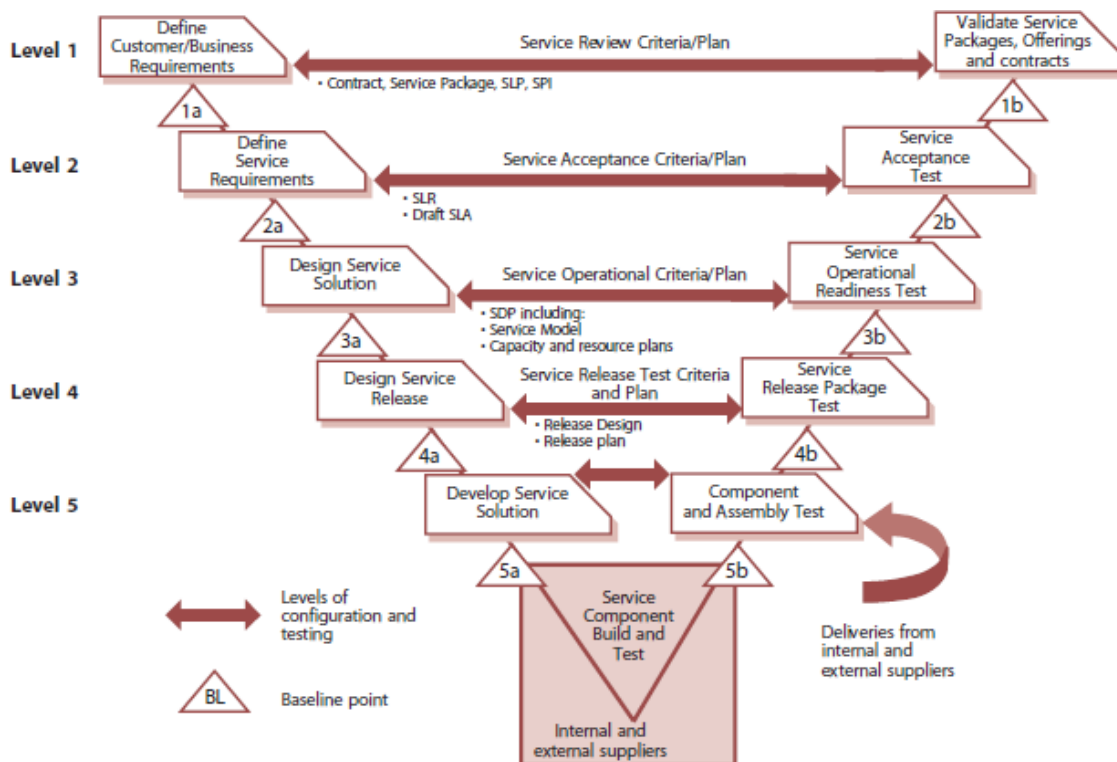
Testy služeb můžeme zpravidla rozdělit do dvou základních kategorií. Prvním typem jsou funkcionální testy, ověřující, zda služba vyhovuje funkční specifikaci, neboli zda jednotlivé funkce služby plní náležité uživatelské požadavky a cíle. Druhou kategorií tvoří skupina nefunkcionálních testů, do které spadají testy dostupnosti, použitelnosti, bezpečnosti, kompatibility, testy proveditelnosti instalace, testy možností zálohování a zotavení služby, výkonnostní, zátěžové a stresové testy, testy operability a údržby služby, aj.

Důležitým pojmem v oblasti testování služeb jsou tzv. regresní testy. Jejich podstata spočívá v tom, že jsou opakovaně testovány části služeb, které nezpůsobily selhání při předchozích testech, ale důvodem pro aplikaci regresních testů je obvykle implementace nové funkcionality nebo změna konfigurace určité služby, apod. Tyto testy zajišťují, že jakákoliv změna ve službě nevyústí v chybu a následné selhání. Typickým příkladem může být detekce špatné spolupráce softwarových komponent, nekompatibility hardwaru či síťových prvků.

Vedle celé řady různých typů testů služeb se proces může zabývat i testováním procesů pro správu služeb, nebo může kontrolovat, zda služba vyhovuje určitým standardům či regulatorním předpisům.

3.3.5.3 V-model

Testovací modely organizují strukturu testovacích aktivit a zpravidla napomáhají podporovat kvalitu služby již na počátku jejího vývoje. Jedním z nejpoužívanějších modelů je tzv. V-model (viz Obr. 8), pomocí kterého jsou konfigurační položky, vytvářené při vývoji služby, uspořádány do několika úrovní. Tento model mapuje na jednotlivé etapy ve vývojovém cyklu příslušné testovací aktivity. Levá strana V-modelu znázorňuje přechod od požadavků zákazníka až po detailní návrh a implementaci služby, pravá strana reprezentuje validaci odpovídajících konfiguračních jednotek definovaných na levé straně modelu.



Obr. 8: Mapování testovacích aktivit na etapy vývoje služby pomocí V-modelu [11]

3.3.5.4 Aktivita a techniky

Správa testů

Správa testů se zabývá řízením a koordinací všech testovacích aktivit a vytvářením testových zpráv o testech. Stará se o správné přidělení prostředků, časové rozvržení testů dle přiřazených priorit a dalších aspektů, správu incidentů a problémů, analýzu a hodnocení testů. Napomáhá rovněž zmírňovat rizika a implementovat potřebné změny.

Plánování a návrh testů

Plánování a návrh testů zahrnuje zajištění zdrojů pro testování - nástroje, osoby s patřičnými dovednostmi, podpůrné služby, apod. Stanovuje také požadavky na finanční prostředky.

Ověření plánu a návrhu testů

Smyslem ověřování plánů a návrhu testů je ujistění, že testovací model splňuje adekvátní pokrytí testů a že testovací skripty jsou úplné a precizně definované.

Příprava testovacího prostředí

Během této aktivity je připravováno prostředí pro testování, testovacím aktivitám jsou přiřazeny potřebné prostředky, včetně vyškolených kompetentních osob či skupin, pro pozdější srovnávání je také zachycena základní konfigurace (configuration baseline) odpovídající počátečnímu stavu testovacího prostředí.

Provádění testů

Testy mohou být prováděny manuálně testerem, který postupně vykonává kroky stanovené v testovacím scénáři, nebo automatizovaně s využitím předpřipravených skriptů a příslušného nástroje. Veškeré výsledky testů jsou průběžně zaznamenávány a příčiny selhání jsou řádně dokumentovány.

Vyhodnocení ukončovacích kritérií a vytvoření zprávy o testech

Pro každý test musí být před jeho spuštěním definována výstupní kritéria, která určují, zda služba splňuje požadovanou úroveň kvality a zda vyhovuje dříve definovaným funkčním požadavkům. Skutečné výsledky jsou porovnávány s očekávanými výsledky testů a je vytvořena zpráva o testech, která shrnuje výsledky a poskytuje stručný přehled nad vykonanými testy.

Návrat do původního stavu a uzavření

V rámci této aktivity je testovací prostředí navraceno do původního stavu a jsou identifikována všechna možná vylepšení služby a dalších testovacích procedur.

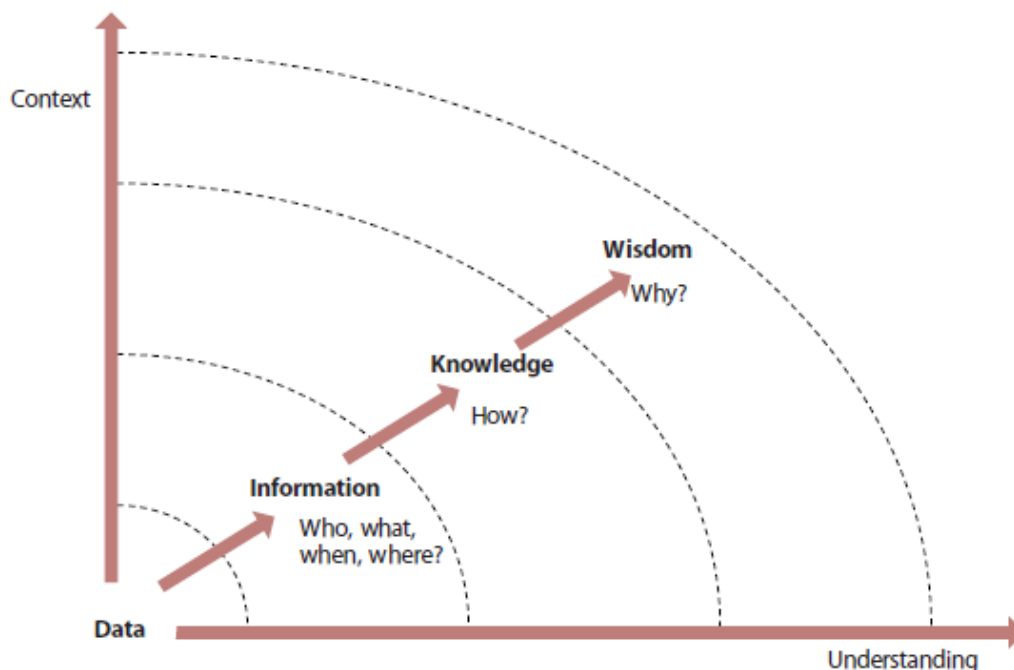
3.3.6 Knowledge Management

Hlavní cílem procesu Knowledge Management je umožnit managementu organizace zlepšit kvalitu rozhodování a usnadnit řešení problémů tím, že budou k dispozici relevantní, spolehlivé, důvěryhodné informace a data, a to během celého životního cyklu služby. Jinými slovy, proces zajišťuje, že ve správný okamžik a na patřičném místě budou kompetentní osobě poskytnuty adekvátní a korektní informace. Proces je odpovědný za sběr, analýzu, uložení a sdílení znalostí a informací v organizaci.

Správa znalostí je významná především ve fázi Service Transition, jelikož znalosti jsou jedním z klíčových částí služby, které se účastní přechodu služby do produkce. Uživatelé, service desk a zaměstnanci podpory musí zcela porozumět různým aspektům nové či změněné služby, musí se adaptovat na novou verzi a získat určité povědomí o používání služby.

Proces je založen na struktuře Data-to-Information-to-Knowledge-to-Wisdom (DIKW), pomocí které jsou surová nepoužitelná data přetvářena a zestručněna na fakta, která mají pro organizaci daleko větší hodnotu a užitek. Daty jsou míněny samostatné, nesouvisející údaje o určitých událostech. Data jsou uložena v příslušných databázích a spravována patřičnými systémy. Informace spojují data do určitého kontextu a jsou obvykle uloženy v částečně strukturovaných dokumentech, e-mailech, popř. dalších médiích. Znalosti (Knowledge) jsou založeny na analýze a slučování informací, spojují informace dále do širších souvislostí a reprezentují je v použitelnější formě. Jsou ovlivněny zkušenostmi, myšlenkami a posouzením

jednotlivců. Nakonec se údaje dostanou do podoby obecného povědomí (Wisdom), které umožňuje cenné informace využít v praxi a uplatnit při rozhodování (viz Obr. 9).



Obr. 9: Struktura DIKW – spojení dat do souvislostí a umožnění lepšího rozhodování [11]

3.3.6.1 Důležité pojmy

Service Knowledge Management System – SKMS

Základem procesu je systém pro správu znalostí (SKMS). Ten se opírá o značné množství dat, která jsou uložena v centrálním úložišti nebo jsou pod kontrolou systému pro správu konfigurací (CMS), který přistupuje k databázi CMDB. CMDB je zásobárnou dat pro CMS, CMS poskytuje vstup pro SKMS a tímto systémem je podporován proces rozhodování.

Service Knowledge Management System nepokrývá pouze informace o prvcích infrastruktury a vztazích mezi nimi, ale je založen na širším konceptu. Obsahuje například údaje vypovídající o úrovních zkušeností zaměstnanců, na základě kterých jsou obsazovány role v procesech, vědomosti o počtech a typech uživatelů (vhodné pro přidělování licencí), údaje o výkonnosti organizace, informace o požadavcích dodavatelů a obchodních partnerů, aj.

3.3.6.2 Aktivita a techniky

Strategie správy znalostí

Na počátku procesu je stanovena strategie, která pojednává o politikách, procedurách, metodách, technologiích a dalších prostředcích použitých ve správě znalostí. Dále strategie popisuje role a odpovědnosti, financování a obvykle v ní jsou zmíněny i plánované organizační změny.

Přenos znalostí

Tato aktivita zajišťuje přenos znalostí k osobám, které je vyžadují. K tomuto účelu existuje mnoho technik. Jednou z těchto technik je vizualizace znalostí, při které se uplatňují různé vizuální prvky, jako jsou např. obrázky, diagramy, náčrtky, obrázkové scénáře (storyboards). Dalšími používanými metodami jsou pořádání seminářů, webových konferencí (webinars) nebo využití komunikačních kanálů a informačních tiskovin, jako jsou noviny či bulletin. Při přesunu znalostí na konkrétní osoby by se měly zohlednit jejich rozličné návyky a styly učení, které se budou odvíjet od jejich věku, povahy a názorů.

Správa dat a informací

Znalosti jsou závislé na kvalitní správě informací a dat, na kterých jsou informace založeny. V rámci této aktivity jsou stanoveny požadavky na data a informace, je definována informační architektura vyhovující požadavkům, jsou formulovány a zavedeny procedury pro efektivní řízení a podporu správy znalostí. Požadavky se týkají obsahu, typu, formátu informačních položek a dalších aspektů. Pojednávají o ochraně dat, bezpečnosti, diskrétnosti, vlastnictví, přístupových právech atd.

Používání systému pro správu znalostí (SKMS)

Odpovědností poskytovatele služeb je vyvinout a spravovat SKMS systém, který vyhovuje všem informačním požadavkům. Systém musí být k dispozici všem zainteresovaným stranám. Pracovníci Service Desku a dalších úrovní podpory tvoří základní centrální bod organizace pro shromažďování informací, které jsou získávány v rámci každodenní správy služeb. Tyto informace jsou řádně dokumentovány a zaznamenávány. Důležitými odběrateli těchto informací jsou pak například pracovníci Problem Managementu.

3.3.7 Evaluation

Proces Evaluation poskytuje standardizované prostředky pro důsledné vyhodnocování změn a objektivní posuzování výkonu služeb. Predikovaný a skutečný výkon služby je posuzován v souvislosti s požadovaným výkonem (dle tzv. akceptačních kritérií) a veškeré odchylky jsou řízeny zákazníkem nebo jeho zástupcem, který může změny akceptovat či nikoliv. Evaluace je důležitá například pro proces Change Management, kterému napomáhá rozhodovat, zda bude změna schválena či nikoliv. Vytváří také důležitý vstup procesu Continual Service Improvement a umožňuje budoucí zdokonalování vývoje služby a správy změn.

3.4 Service Operation

Přestože mohou být procesy v organizaci precizně navrženy a důkladně implementovány, nebudou přinášet zákazníkovi užitečnou hodnotu, pokud nebude vykonávání jednotlivých aktivit dobře organizováno. Bez kvalitních operativních procesů, shromažďování dat a měření také není možné poskytované služby vylepšovat.

Hlavním cílem fáze Service Operation je koordinace a plnění aktivit a procesů, které poskytují a řídí služby poskytované zákazníkům a uživatelům. Je zodpovědná za efektivní fungování komponent sloužících pro podporu služeb, optimalizaci ceny a kvality služby.

Všechny funkce, procesy a aktivity jsou navrženy tak, aby podporovaly poskytování služby na předem stanovené a dohodnuté úrovni. Nicméně, služby jsou poskytovány v neustále se měnícím prostředí a je nutné vypořádat se s přicházejícími změnami v byznysu či v prostředí technologií. Snahou organizace v rámci Service Operation je docílit určité rovnováhy mezi protikladnými aspekty a prioritami.

Zásadním problémem, který se objevuje nejen ve fázi Service Operation, ale i v ostatních fázích životního cyklu služby, je udržení rovnováhy mezi externím a interním pohledem na IT. Externí pohled vychází ze zkušeností uživatelů a zákazníků se službou. Uživatelé a zákazníci se obvykle nestarají o takové detaily, jakým způsobem je služba poskytována a řízena, jaká technologie je použita pro správu služeb apod. Jediným jejich zájmem je požadovaná a domluvená kvalita služby. Interní pohled se naopak zaměřuje na způsob, jakým jsou jednotlivé IT komponenty a systémy řízeny. Je nutno podotknout, že oba pohledy jsou důležité. Organizace, která se zaměřuje pouze na požadavky byznysu a nemá důkladně promyšlený způsob, jakým budou služby poskytovány, pravděpodobně nebude schopna naplnit požadavky uživatelů. Naopak organizace, která se bude nadměrně soustředit na interní systémy a technologie poskytování služeb, aniž by plnila reálné požadavky uživatelů, nepochybně docílí pouze drahých služeb s velmi nízkou užžitnou hodnotou pro zákazníka.

Dalšími problémy v souvislosti s operativními procesy může být udržení rovnováhy mezi kvalitou a cenou služby, reaktivním a proaktivním managementem aj.

Procesy fáze Service Operation:

- ☐ Event Management
- ☐ Incident Management
- ☐ Problem Management
- ☐ Request Fulfilment
- ☐ Access Management

Jednotlivé procesy z kapitoly Service Operation jsou podrobně popsány v publikaci „Service Operation“. [12]

3.4.1 Event management

Event management, tedy správa událostí, je jedním z klíčových procesů operativní fáze. Tento proces se zabývá sledováním a zachytáváním událostí a změn stavu, které se vyskytly v rámci IT infrastruktury a které mají vliv na správu IT infrastruktury nebo poskytování služeb. Správa událostí úzce souvisí s monitoringem, nemůžeme však tvrdit, že monitoring a Event management jsou totožné pojmy. Zatímco Event management spočívá v tom, že zachytává oznámení o události v momentě jejího výskytu, princip monitoringu je založen na tom, že kontroluje stav zařízení, i když se žádná událost v souvislosti s daným zařízením nevyskytla.

3.4.1.1 Využití správy událostí

Správa událostí může být použita k různým účelům. Především se aplikuje na tzv. konfigurační položky (CI). Kromě aplikace na monitorování konfiguračních jednotek se setkáváme také s aplikací správy událostí na sledování použití softwarových aplikací, monitoring výkonu serveru, k různým bezpečnostním opatřením v rámci IT infrastruktury nebo také pro detekci požáru a kouře.

3.4.1.2 Aktivita a techniky

Vznik a oznámení události

Celý proces správy událostí je nastartován v okamžiku, kdy se nějaká událost vyskytne. Předem by tedy mělo být jasno, co všechno by mělo být monitorováno, kdy a za jakých předpokladů bude vygenerována příslušná událost, kde se budou informace o událostech zaznamenávat, ukládat apod. Velkým přínosem je, když jednotlivé konfigurační položky mají v sobě již zabudovány vlastní mechanismus pro generování událostí a to platí i pro softwarové aplikace.

Pokud se u konfigurační položky vyskytla nějaká událost, vygeneruje se oznámení o události a dojde k zachycení informace příslušným nástrojem, který je k tomu určený. Zde je důležité, aby oznámení obsahovalo smysluplné informace tak, aby bylo možné učinit následná rozhodnutí, co s danou událostí provést a kdo je za příslušnou akci zodpovědný. Jednotlivé zodpovědnosti a role by měly být důkladně stanoveny již v předchozích fázích – Service Design a Service Transition.

Filtrování a třídění událostí

Jakmile je událost zachycena, přijde na řadu filtrování událost. Filtrováním určujeme, zda bude daná událost předána nástroji pro správu událostí nebo bude ignorována a zapsána pouze do souboru, tzv. logu. Filtrace je užitečná, když například potřebujeme, aby bylo odchyceno pouze první z řady opakujících se oznámení o stejné události.

Stěžejní aktivitou v rámci tohoto procesu je rovněž roztřídění událostí dle jejich typu. V zásadě rozlišujeme tři základní typy událostí:

☐ Informační událost

Informační událost slouží pouze k informačnímu účelu a nevyžaduje žádnou následnou aktivitu. Využívá se zejména k zjištění stavu zařízení nebo služby, k ověření úspěšného dokončení nějaké aktivity nebo také ke statistickým účelům (např. zjištění počtu uživatelů přihlášených do určité aplikace).

❑ Výjimka

Pokud byla vyvolána výjimka, znamená to, že nějaké zařízení nebo služba nefunguje tak, jak by fungovat mělo. Dojde k totálnímu selhání nebo narušení funkčnosti, popř. rapidnímu snížení výkonu zařízení či služby. Typickou událostí, kterou zařazujeme do typu výjimky, je situace, kdy selže server z důvodu zahlcení nebo kdy stoupne doba odezvy v síti pro danou akci, např. nad 5 vteřin.

❑ Varování

Varování výrazně přispívá k předcházení výjimky, která by mohla nastat v důsledku toho, že některá vlastnost určitého zařízení nebo služby přesáhla povolený práh. Jedná se tedy o preventivní opatření a oznamuje příslušným osobám nebo nástrojům, že by mělo dojít ke kontrole stavu konkrétní položky a následným opatřením. Příkladem varování by mohla být událost, kdy se na serveru zvýší využití paměti nad určitou hranici a další zvyšování nároků na paměť by mohlo způsobit výrazné zvýšení doby odezvy.

Korelace a výběr odpovědi

V těchto krocích dochází k rozpoznání typu události, zjištění její významnosti a rozhoduje se zde, jak se s událostí vypořádat. Stěžejní aktivitou v rámci korelace je analýza, pomocí které usilujeme o nalezení původu události (z angličtiny „root cause analysis“). Tato analýza je založena na hledání vzájemných souvislostí mezi událostmi a snaží se zjistit, zda by některé události nemohly být vysvětleny jinými.

V okamžiku, kdy je daná událost rozpoznána, dojde k vyvolání odpovědi, kterou má na starost tzv. spouštěč. Ten iniciuje následný úkol, který danému typu události přísluší. Existuje mnoho typů reakcí na události a každá organizace může zacházet s událostmi rozdílným způsobem v závislosti na jiných zvyklostech, odlišných technologiích použitých v organizaci apod. Uvedme si proto pouze základní možnosti odpovědí na události, které se v procesu Event Management využívají nejčastěji:

❑ Automatická odpověď

Automatická odpověď je založena na předchozích zkušenostech s řešením určitých případů, tedy na předem známých událostech, u kterých je možné následnou reakci automatizovat. Můžeme zde zařadit automatický restart zařízení nebo služby, uzamčení aplikace z důvodu znemožnění přístupu neautorizovaným uživatelům aj.

❑ Záznam události do logu

Typickým příkladem, kdy je postačující pouze zaznamenat událost, je informační událost, která nám sděluje nějakou informační zprávu o zařízení či službě a není kritická pro ostatní komponenty IT infrastruktury, popř. pro celý proces poskytování IT služeb. Informační události pak postupují do dalších procesů, jako jsou Backup Management a Storage Management.

❑ Zásah příslušné osoby

Někdy nastane situace, kterou je nutno vyřešit v určitém časovém intervalu a neexistuje pro ni žádná automatická aktivita. Obvykle se jedná o opravu specifického zařízení, kde je nutný zásah kompetentní osoby, popř. týmu. Příslušné osobě je potřeba zásahu

oznámena, včetně předání informací o dané události a dalších referencí potřebných k nápravě, jako je uživatelská příručka apod.

❑ Vstup do Incident, Problem nebo Change Managementu

U některých případů vstupuje událost do dalších procesů, jako je Incident, Problem nebo Change Management. Může se také jednat o kombinaci zmíněných procesů. Jako příklad si uveďme situaci, kdy byla ve firemní síti nalezena nová zařízení, aniž by byla předem učiněna jejich autorizace. Tyto změny je tedy žádoucí provést pomocí procesu Change Management, a proto je vzniklá událost předána tomuto procesu.

Ověření a uzavření události

Na závěr celého procesu je nutno provést ověření a celkové uzavření události. Je zřejmé, že pokud je denně generováno velké množství událostí, není ve většině případů možné ověřit každou z nich. V takovýchto případech je důležité se zaměřit alespoň na ty nejvýznamnější, především je podstatné ověřit, zda byly zvládnuty všechny výjimky. Nakonec se celá událost uzavře, pokud všechny aktivity proběhly v pořádku. Nicméně, některé události zůstávají otevřené delší dobu, jelikož vstupují do jiných procesů nebo čekají na pozdější událost, která by je uzavřela.

3.4.2 Incident Management

Dalším velice důležitým procesem v rámci fáze Service Operation je Incident Management. Za incident můžeme považovat jakékoliv neplánované narušení poskytované IT služby nebo snížení její kvality. Cílem tohoto procesu je tedy zaznamenávat a řešit incidenty a co nejrychleji obnovit normální stav služby. [10]

3.4.2.1 Service Desk

Service Desk je organizační jednotkou, která je životně důležitá pro IT oddělení organizace a slouží jako komunikační kanál mezi poskytovatelem služeb a zákazníkem. Jednotlivé poruchy, připomínky a námitky týkající se služeb mohou být ohlášeny koncovými uživateli prostřednictvím telefonního hovoru nebo webového rozhraní pro reporting incidentů. Jiným způsobem oznámení incidentu je pomocí již zmíněného Event Managementu, monitorováním konfiguračních položek a dalších objektů. Kromě uživatelů mohou incidenty ohlásit rovněž techničtí pracovníci v organizaci.

Service Desk v podstatě utváří vnější dojem na celou organizaci. Dobrý Service Desk může vykompenzovat nedostatky kdekoli uvnitř organizace, zatímco špatně fungující Service Desk může vytvořit špatný dojem i na vcelku efektivní IT organizaci.

Cíle Service Desku

Prvořadým cílem Service Desku je obnovit normální stav služby v co nejkratším čase. Činnost této jednotky může spočívat v napravení technické chyby, splnění požadavku uživatele nebo pouze v zodpovězení dotazu, který umožní uživateli pokračovat ve využívání dané služby.

Hlavní zodpovědnosti Service Desku:

- ☐ Zaznamenávání všech detailů o incidentech nebo požadavcích, kategorizace a stanovení priority incidentů
- ☐ Poskytnutí tzv. first-line diagnostiky
- ☐ Řešení incidentů a požadavků, které je Service Desk schopný řešit
- ☐ Informování uživatele o vývoji incidentu či požadavku, oznámení blížících se změn nebo očekávaných výpadků
- ☐ Uzavírání všech vyřešených incidentů a požadavků
- ☐ Provádění uživatelských průzkumů ohledně spokojenosti se službami

3.4.2.2 Aktivita a techniky**Záznam, kategorizace a stanovení priority incidentu**

Proces začíná v momentě, kdy je incident identifikován jedním z výše zmíněných způsobů (viz kapitola 3.4.2.1). V organizaci by měl být kladen velký důraz na to, aby byly monitorovány všechny stěžejní komponenty v rámci IT infrastruktury, aby při výskytu poruchy nebo při odhalení potenciální poruchy mohl být incident vyřešen ještě před tím, než bude mít daná porucha vliv na koncového uživatele.

Každý incident musí být řádně zaznamenán spolu se všemi relevantními informacemi tak, aby bylo možné všechny incidenty v historii zpětně vyhledat. Informace zahrnují takové údaje, jako např. datum a čas výskytu incidentu, naléhavost, způsob oznámení, popis příznaků, priorita incidentu aj. Někdy se v praxi stává, že uživatelé mají speciální požadavky nebo připomínky ohledně poskytované služby, které se netýkají jejího narušení nebo snížení její kvality, a tento požadavek nahlásí pomocí webového rozhraní nesprávně jako incident. Tento postup je nesprávný, protože takovéto požadavky jsou řešeny procesem Request Fulfilment. U reportovaného incidentu je nutné nejprve rozhodnout, zda se jedná o skutečný incident či nikoliv.

Pro snadnější odhalení příčiny jsou incidenty klasifikovány do skupin dle jejich typu. V rámci klasifikace jsou spojovány incidenty se známými chybami a problémy zaevidovanými v databázi. Takovéto spojování umožňuje použít již osvědčená řešení, která nevyžadují další vyšetřování incidentu. Klasifikace nám napomáhá vybrat vhodnou skupinu specialistů, kteří budou daný incident řešit.

Příklad klasifikace incidentu by mohl vypadat následovně:

- ☐ Typ: Chyba/selhání
- ☐ Kategorie: Software
- ☐ Podkategorie: Databáze
- ☐ Poznámka: Uživatel nahlásil chybu SQL dotazu, když se v aplikaci pokusil vyhledat osobu se jménem „Jan Novák“

Po identifikaci a zaznamenání incidentu se obvykle stanovuje jeho priorita. Priorita je stanovována na základě dvou faktorů, kterými jsou naléhavost a dopad incidentu. Dopadem incidentu obvykle rozumíme počet ovlivněných uživatelů, ale nemusí to být nutně pravidlem. Dopad může také souviset s možnými finančními ztrátami, s vlivem na dobré jméno společnosti

apod. Priorita incidentu úzce souvisí s klasifikací, kdy každému typu incidentu může příslušet určitá priorita, ale u neznámých problémů se priorita zpravidla určuje dle následující tabulky.

Priorita incidentu		Dopad		
		Vysoký	Střední	Nízký
Naléhavost	Vysoká	1	2	3
	Střední	2	3	4
	Nízká	3	4	5

Tabulka 1: Stanovení priority incidentu

Výsledná priorita, kterou je možno vyčíst z tabulky, pak určuje dobu, během které musí dojít k vyřešení incidentu. Například incidenty s výslednou prioritou 1 by měly být vyřešeny do jedné hodiny, zatímco incidenty s prioritou 3 do jednoho dne.

Počáteční diagnóza, eskalace incidentu a další diagnózy

V případě, že je incident ohlášen telefonním hovorem, nastává fáze počáteční diagnózy. Snahou Service desku je odhalit všechny symptomy incidentu a díky dřívějším informacím o již známých chybách se pokusit incident vyřešit bez pomoci dalších stran.

Pokud není v silách Service Desku obnovit stav služby přímo při hovoru s uživatelem nebo do určité doby po hovoru, incident se dostává do fáze tzv. zvýšeného úsilí, v oficiální publikaci ITIL je označován tento krok jako eskalace incidentu („incident escalation“). Incident je předán k vyřešení specializované skupině pro podporu služeb, která má hlubší technické znalosti o řešení konkrétního incidentu. Z hlediska organizace může být daná skupina interní nebo externí. Externí skupinou může být softwarový dodavatel nebo výrobce hardwarových komponent. Skupina, které byl incident předán, se dále zabývá diagnózou incidentu, zkoumáním jeho příčiny, porovnáním incidentů s dřívějšími, které jsou uloženy v databázi apod.

Vyřešení a uzavření incidentu

Po nalezení potenciálního řešení dojde k jeho aplikaci na danou službu. Způsob vyřešení je závislý na charakteru incidentu. Service Desk může provést implementaci řešení centrálně (např. restart serveru) nebo vzdáleně pomocí určitého nástroje pro vzdálenou správu. V jednodušších případech je možno požádat uživatele, aby danou akci provedl na své pracovní stanici sám dle instrukcí. Řešení může být také svěřeno týmu specializovaných odborníků (např. změna konfigurace serveru aj.).

Jakmile je incident vyřešen a jsou splněny veškeré požadavky uživatele v souvislosti s daným problémem, může být incident uzavřen. Po uzavření by měli pracovníci Service Desku provést kontrolu, zda byly všechny detaily incidentu řádně dokumentovány pro pozdější využití. Mělo by být rozhodnuto, zda budou zapotřebí nějaká preventivní opatření, aby se v budoucnu neopakoval podobný incident. Při uzavírání se obvykle ještě vytvoří opětovná klasifikace incidentu dle typu. Důvodem je to, že při počáteční diagnóze je většinou uživatel schopen popsat pouze příznaky incidentu, nikoliv konkrétní problém, který incident způsobil. Iniciální a závěrečná klasifikace se proto mohou lišit.

3.4.3 Problem Management

Problém můžeme definovat jako příčinu jednoho či více incidentů. V momentě vytvoření záznamu o problému příčinu neznáme. Za vyšetření a vyřešení příčiny je zodpovědný proces Problem Management. Záměrem správy problémů je předcházet vzniku nových problémů, eliminace opakujících se incidentů a minimalizace dopadu incidentů, kterým nelze předcházet. Z hlediska byznysu přináší tento proces větší dostupnost poskytovaných služeb. [10] Řešení problémů je často zajištěno mechanismy a aktivitami procesů Change Management a Release Management. Přestože jsou Incident Management a Problem Management separátními procesy, využívají podobné přístupy a nástroje, jelikož spolu úzce souvisí.

3.4.3.1 Aktivita a techniky

Detekce a záznam problému

Vznik problému může být iniciován různými způsoby. Může se stát, že Service Desk vyřeší určitý incident, ale není schopen určit jeho jednoznačnou příčinu. Aby se podobný incident již v budoucnu neopakoval, je nutné vytvořit záznam o problému a daný problém odstranit. Další možnost vzniku problému pramení ze zachycení události pomocí nástroje pro správu událostí. Tento nástroj automaticky vyvolá incident a pro zjištění jeho příčiny musíme opět předat iniciativu procesu Problem Management. Nutnost vzniku problému může také nastat při oznámení dodavatele o existenci určitého problému nebo při analýze incidentů v proaktivním managementu.

Všechny vzniklé problémy musí být řádně zaznamenány s veškerými relevantními informacemi a s odkazy na incidenty, které způsobily jejich vyvolání. Záznam o problému zahrnuje podrobné informace o uživateli, službě, zařízení, dále prioritu a kategorizaci, popis incidentu a detaily o již provedené diagnóze.

Klasifikace problému a stanovení priority

Kategorizace problémů je totožná s kategorizací incidentů, stejně jako stanovení priorit. Stanovení priorit problémů je často ovlivněno i jejich vážností. Vážnost v podstatě udává míru důležitosti z pohledu infrastruktury. Zaměřujeme se na otázky, zda může být systém zotaven nebo musí být nahrazen, jak dlouho bude trvat náprava problému, kolik konfiguračních jednotek je daným problémem ovlivněno apod. Tyto aspekty mohou ovlivnit výslednou prioritu problému.

Diagnóza a vyšetřování problému

Podstatou vyšetřování incidentu je nalezení jeho původní příčiny. Charakter vyšetřování je ovlivněn několika faktory – závažností, naléhavostí a dopadem problému na organizaci. Během této aktivity je obvykle využívána databáze známých chyb (KEDB) a různé techniky srovnávání problémů, jako například vyhledávání problému dle klíčových slov, aby bylo možné zjistit, zda už se problém někdy v minulosti nevyskytl.

Existuje velké množství diagnostických metod a technik. Nicméně, alespoň pro představu si uveďme jen některé z nich:

❑ Chronologická analýza (Chronological Analysis)

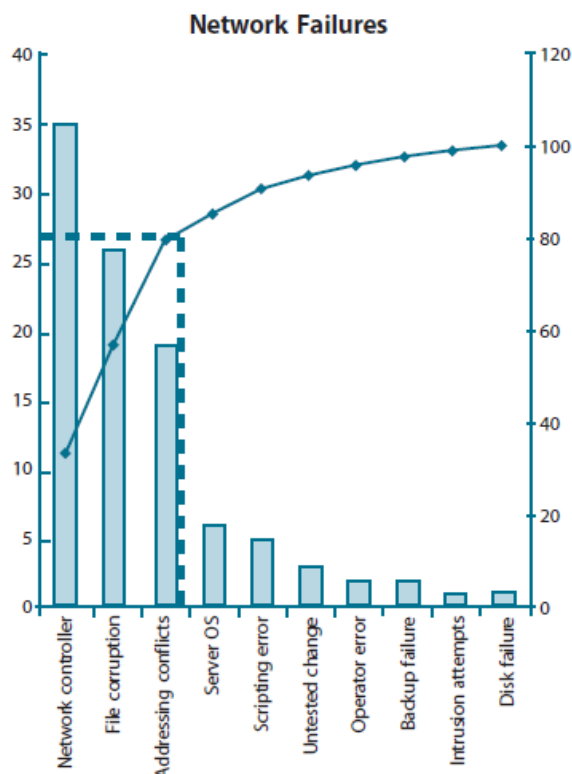
Tato analýza je založena na sestavení časové linie událostí, která znázorňuje všechny události v chronologickém pořadí. To nám například umožňuje odhalit problémy, které byly vyvolány jinými a zjistit tak původní příčinu daného problému (root cause).

❑ Analýza hodnoty bolesti (Pain Value Analysis)

Pomocí této metody můžeme rozpoznat incidenty a problémy, které způsobují organizaci největší bolest, resp. metoda se zaměřuje na zjištění dopadu incidentů a problémů na organizaci. Při zjišťování dopadu se přihlíží k počtu ovlivněných zákazníků (popř. uživatelů), době nefunkčnosti služby a rovněž k odhadovaným nákladům. Přednost při řešení problémů pak dostanou ty problémy, které způsobují největší dopad na organizaci.

❑ Paretova analýza (Pareto Analysis)

Pomocí této metody jsme schopni oddělit důležité potenciální příčiny od triviálních. Postup analýzy spočívá v tom, že sestavíme tabulku příčin, u každé z nich uvedeme procento odpovídající frekvenci jejího výskytu (relativní četnost výskytu) a řádky seřadíme sestupně dle této četnosti. Následně řádky doplníme o kumulativní četnost výskytu a obě veličiny zakreslíme do grafu. Relativní četnost je vhodné reprezentovat sloupcovým a kumulativní četnost spojnicovým grafem. Nakonec do grafu zakreslíme rovnoběžku s osou x a druhou rovnoběžku s osou y v bodě, ve kterém je hodnota kumulativní četnosti výskytu rovna osmdesáti procentům. Vzniklá oblast vymezuje sloupce zahrnující nejdůležitější příčiny, na které by měl být kladen největší důraz. Na obrázku (viz Obr. 10) je vidět ukázka Paretovy analýzy pro odhalení příčin selhání sítě.



Obr. 10: Oddělení důležitých příčin od triviálních pomocí Paretovy analýzy [12]

Workaround a vytvoření záznamu o známé chybě

Někdy se stává, že existuje určité prozatímní řešení problému, které umožní vypořádat se s daným problémem. Například při selhání programu z důvodu poškozeného vstupního souboru, může být soubor ručně upraven tak, aby dokončení programu proběhlo úspěšně. Toto dočasné řešení nazýváme „workaround“. Je však důležité, aby příčina problému byla později odstraněna natrvalo, aby se daný problém v budoucnu neopakoval.

Jakmile je dokončena diagnóza problému, nalezena jeho původní příčina (root cause) a popřípadě je aplikováno dočasné řešení, musí být vytvořen záznam o známé chybě (Known Error) a uložen do databáze známých chyb (Known Error Database). V případě, že se v budoucnu objeví podobné incidenty a problémy, může být služba díky údajům v této databázi obnovena mnohem rychleji.

Vyřešení a uzavření problému

V tomto kroku aplikujeme nalezené řešení na reálný problém. Může se stát, že je potřeba provést určité změny ve funkcionalitě poskytované služby a proto jsme povinni vyvolat RFC. Předtím než dojde k aplikaci řešení, musí být požadavek na změnu odsouhlasen. Schválení požadavku na změnu má za úkol proces Change Management.

Po úspěšném dokončení změny a aplikaci řešení musí být záznam o problému formálně uzavřen, stejně jako všechny související incidenty, které zůstaly otevřené. Rovněž se aktualizuje stav záznamu o známé chybě, pro kterou bylo nalezeno řešení.

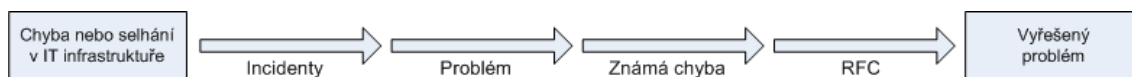
Revize vážnějších problémů

Pokud se jedná o vážnější problém, provede se obvykle nakonec procesu revize problému. Revize slouží k přezkoumání provedených kroků a ke zjištění, které z nich byly provedeny korektně a které byly provedeny naopak nesprávně. Tím nám revize poskytuje návod na to, co by mohlo být v budoucnosti provedeno lépe a jakým způsobem předcházet opakujícím se problémům.

3.4.3.2 Souvislost incidentů, problémů, známých chyb a RFC

Pokud je příčina incidentu zřejmá a jasná, je možné incident vyřešit bez dalšího vyšetřování. V takovýchto případech lze smlouvenou kvalitu služby zákazníkovi obnovit velice rychle, např. restartováním PC. Pokud však neznáme příčinu incidentu, dojde k vytvoření záznamu o problému. Je nutno zmínit, že záznam o problému je nezávislý na záznamech o asociovaných incidentech. Z toho plyne, že vyšetřování problému může přetrvávat i poté, co dojde k uzavření souvisejícího incidentu. Problém obvykle vyústí ve vznik několika incidentů.

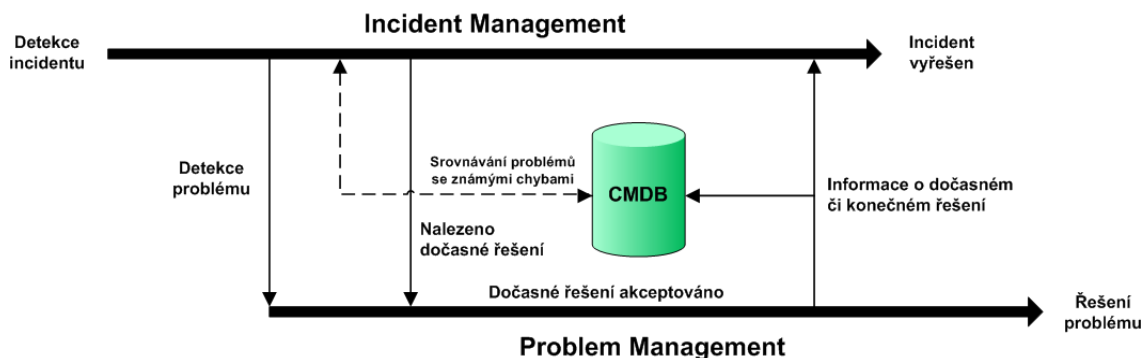
Následující obrázek (viz Obr. 11) znázorňuje přechod od výskytu chyby k vyřešenému problému.



Obr. 11: Přechod od výskytu chyby v IT infrastruktuře k vyřešenému problému

Během řešení incidentu je incident srovnáván s databází známých chyb (viz Obr. 12). Pokud je v databázi nalezeno řešení nebo workaround, může být bezprostředně aplikováno.

Pokud tomu tak není, Incident Management je zodpovědný za nalezení dočasného či úplného řešení, které pak Problem Management analyzuje a aktualizuje příslušný záznam o problému. Může také dojít k tomu, že řešení problému objeví právě Problem Management. V tomto případě je Incident Management informován o změně stavu incidentu na „uzavřený“ či „známá chyba“.



Obr. 12: Spolupráce Incident a Problem Managementu

3.4.4 Request Fulfilment

Rámec ITIL ve své třetí verzi přináší několik novinek a vylepšení v řízení IT infrastruktury. Jednou z odlišností od předchozí verze rámce je oddělení správy uživatelských požadavků od procesu Incident Management a zavedení nového procesu Request Fulfilment, který se těmito požadavky zabývá.

Většinou se jedná o menší žádosti, informace, rady nebo standardní změny v souvislosti s poskytovanou službou. Společnými znaky těchto požadavků je nízká cena, nízké riziko a vysoká frekvence. Proto je lepší nezahrnout jejich správu pod procesy Incident a Change Management, ale provádět ji zvláštním procesem. Příkladem požadavku může být žádost o změnu hesla, dodatečná instalace softwaru na pracovní stanici či žádost o prodloužení platnosti licence.

3.4.4.1 Service Request vs. Incident

Rozdíl mezi incidentem a požadavkem na službu (Service Request) spočívá v tom, že incidentem obvykle označujeme neočekávanou událost, která narušuje nebo by mohla narušit kvalitu služby, zatímco požadavek může být očekávatelný, měl by být plánovaný a obvykle nesouvisí s kvalitou služby.

3.4.4.2 Aktivita a techniky

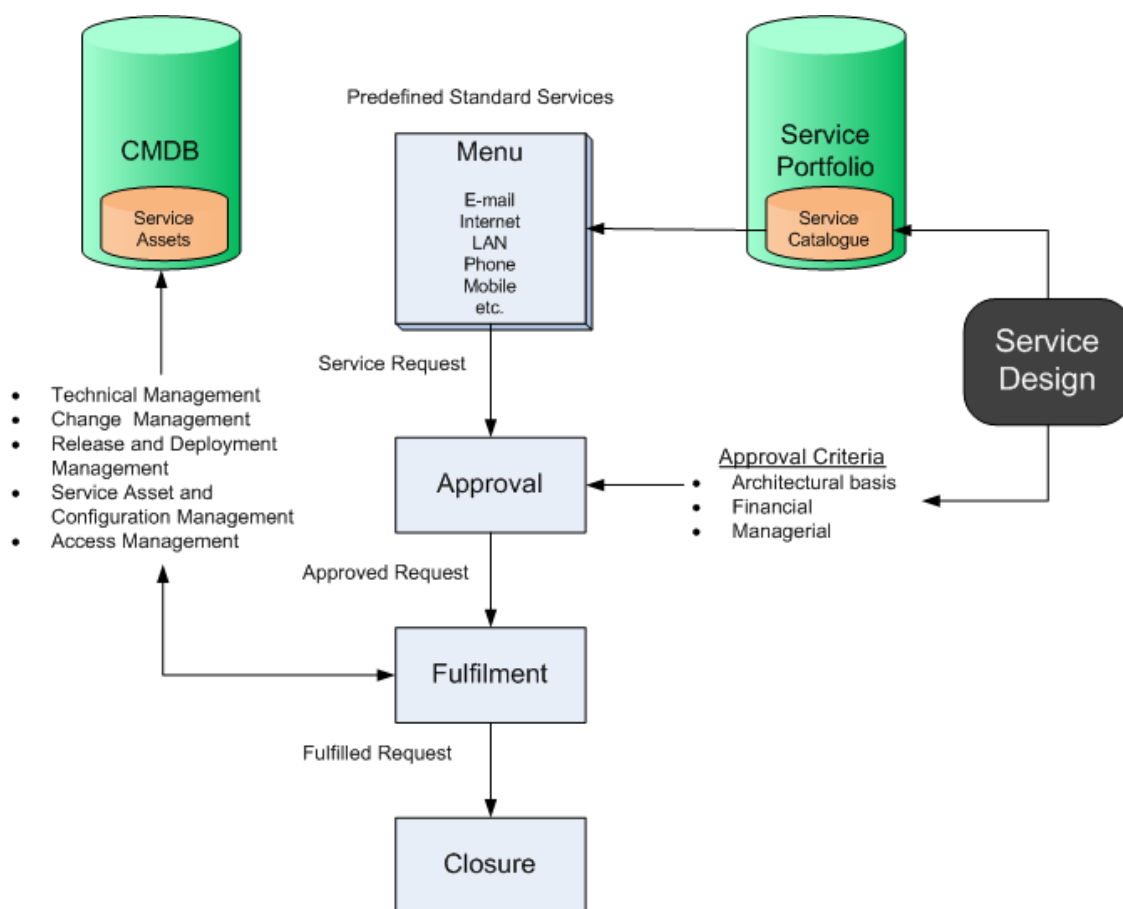
Volba požadavku

K vygenerování požadavku na službu uživatelům napomáhají speciální technologie, které jsou svázány s nástroji Service Managementu. Uživatelům je obvykle přes webové rozhraní nabídnuta volba typu požadavku z tzv. Service Menu s možností vyplnit patřičné detaily. Service Menu je seznam dobře známých služeb, které byly navrženy pro běžné rutinní potřeby. Tyto služby jsou zaznamenány v databázi Service Catalogue, podobně jako všechny ostatní, tzv. live IT služby.

Finanční schválení a splnění požadavku

Předtím, než dojde k plnění požadavku, se musí požadavek schválit dle různých kritérií. V rámci aktivity schvalování musí být uživatelem odsouhlaseny náklady na splnění požadavku. Následným krokem je již samotné plnění požadavku. Některé jednodušší žádosti mohou být provedeny Service Deskem, jiné, zejména ty složitější, jsou obvykle předány specialistům či dodavatelům. Nicméně, uživatel by měl být neustále informován o průběhu plnění požadavku. Plnění požadavku zajišťuje proces Technical Management a za provádění příslušných akcí odpovídají procesy fáze Service Transition, jako např. Change Management, Service Asset and Configuration Management apod. Po splnění je požadavek odkázán zpět Service Desku k ověření, zda je uživatel spokojen s výsledkem a následnému uzavření.

Následující obrázek (viz Obr. 13) znázorňuje proces Request Fulfilment.



Obr. 13: Princip procesu plnění uživatelských požadavků

3.4.5 Access Management

Access Management (správa přístupů) je dalším operativním procesem, pomocí kterého je řešen jeden z aspektů bezpečnosti v organizaci. Hlavním úkolem Access Managementu je poskytovat přístupová práva uživatelům a umožnit jim tak přístup k využívání určité služby či skupiny služeb. Na druhou stranu proces zamezuje přístup ke službám neautorizovaným uživatelům, tedy uživatelům, kteří k službě přistupovat nesmějí. Ve skutečnosti se jedná o vykonávání akcí, které byly stanoveny v procesech Security Management a Availability

Management. Availability Management zajišťuje, že uživatelé mají přístup k službě během celé smlouvané doby. Řízení přístupu k službám pomáhá budovat důvěrnost, dostupnost a integritu informací v organizaci.

3.4.5.1 Důležité pojmy

Access (přístup)

Přístup lze definovat jako rozsah nebo úroveň funkcionality služby či dat, které je uživatel oprávněn využívat.

Identity (identita)

Identitou definujeme každou osobu v organizaci, která je oprávněná k přístupu k daným službám nebo informacím. Mezi tyto osoby můžeme zařadit zaměstnance, zákazníky, dodavatele, prodejce aj. Identita je specifikována různými informacemi o daném člověku. Informace obvykle zahrnují základní údaje o osobě jako jméno, adresa, kontaktní údaje, apod. Kromě toho však mohou obsahovat i biometrické údaje (otisky prstů, DNA), které napomáhají zajistit unikátnost identity.

Rights (práva)

Právem rozumíme nastavení, díky kterému je poskytnuta uživateli různá úroveň přístupu k službě nebo ke skupině služeb. Mezi typická práva patří právo pro čtení, zápis, spouštění, změnu či smazání.

Service groups (skupiny služeb)

V mnoha případech uživatelé nepřistupují pouze k jedné službě, ale uživatelé provádějící podobné aktivity využívají podobné služby. Díky zavedení skupiny služeb není třeba jednotlivým uživatelům udělovat přístupy zvlášť ke každé službě, ale skupina uživatelů může získat přístup k celé množině služeb, které je oprávněna využívat.

Directory Services

Directory Services je pojem, kterým označujeme specializovaný nástroj určený pro správu přístupů a práv.

3.4.5.2 Aktivita a techniky

Žádost o přístup ke službě a verifikace

Změna přístupu k službě může být uskutečněna například při povýšení, přesunu či odchodu zaměstnance, podáním žádosti Service Request přes tzv. Request Fulfilment System nebo pomocí RFC.

Po podání žádosti následuje verifikace, která se skládá ze dvou kroků – autentizace a autorizace. Autentizací ověřujeme, zda žádající uživatel je opravdu tím, za koho se vydává. Autentizace se obvykle realizuje pomocí uživatelského jména a hesla, popřípadě porovnáním biometrických údajů a využitím jiných bezpečnostních technik. Autorizací pak ověřujeme, že uživatelská žádost o využívání dané služby je oprávněná.

Přidělování práv

Následující aktivitou je samotné přidělení uživatelských práv. Je nutno podotknout, že rozhodování o tom, kdo bude mít přístup k jaké službě, není součástí tohoto procesu. Tyto politiky a předpisy jsou definovány již v předchozích fázích – Service Strategy a Service Design. Podstatou Access Managementu je poskytování, resp. omezování práv uživatelům, uživatelským rolím a skupinám.

Změny stavu identit a monitoring přístupů

Vzhledem k tomu, že se v organizaci mohou měnit role uživatelů, musí se v těchto případech nutně změnit i jejich přístupová práva k službám. Změna práv nastává v případě povýšení nebo odstoupení zaměstnance, při přesunu zaměstnance do jiného regionu, při změně pracovní náplně nebo při odchodu zaměstnance do penze. V každé z těchto možností platí jiná pravidla pro změnu přístupových práv. Pokud má daná organizace vytvořený pro každý typ uživatele tzv. životní cyklus uživatele, je možné proces omezování práv při změně stavu identit automatizovat.

Kromě plnění žádostí o přidělení práv se proces zabývá rovněž monitorováním veškerých přístupů k službám a datům v organizaci. Proces je zodpovědný za to, že k daným službám mají přístup předem stanovení autorizovaní uživatelé. Ve spolupráci s procesem Information Security Management a speciálními detekčními nástroji je možno případné neautorizované přístupy uživatelů odhalit a zaznamenat.

Odebrání přístupových práv

Odebrání přístupových práv může být následkem odstoupení, propuštění, smrti uživatele nebo dalších situací, kdy již uživatel přístupová práva nevyžaduje.

3.5 Continual Service Improvement

Continual Service Improvement (CSI) je část ITIL v3, která poskytuje odbornou pomoc při hodnocení a vylepšování kvality služeb a celkové vyspělosti Service Managementu napříč celým životním cyklem služby. CSI zahrnuje metody, techniky a nástroje pro zlepšování procesů a současně také zajištění efektivity nákladů.

Procesy fáze Continual Service Improvement:

- ☐ Service Measurement
- ☐ Continual Service Improvement Process
- ☐ Service Reporting

Jednotlivé procesy z kapitoly Continual Service Improvement jsou podrobně popsány v publikaci „Continual Service Improvement“. [13]

3.5.1 Service Measurement

Monitorování a měření jsou základní podporou CSI a nezbytnou součástí správy IT služeb, a jsou předmětem procesu Service Measurement. Základem pro hodnocení a měření procesů a kvality služeb jsou tzv. metriky. Pomocí metrik jsme schopni změřit výsledek procesu nebo aktivity, porovnáním konkrétního výsledku určitého parametru procesu s jeho předem stanovenou hodnotou. Metrika definuje, co by mělo být měřeno, dále pak specifikuje způsoby měření, přijatelný rozsah výsledků a akce nutné k normalizaci výkonnosti. Například můžeme ověřit, zda byl během jedné hodiny vyřešen určitý počet incidentů. Metrika zpravidla poskytuje kvantitativní data a ta jsou pomocí CSI převáděna na kvalitativní informace. Využívá se zde struktura DIKW, zmíněná v kapitole popisující proces Knowledge Management (viz kapitola 3.3.6), prostřednictvím které jsou data postupně transformována na obecné povědomí (wisdom), které umožňuje správné posuzování a rozhodování. Obecně můžeme metriky rozdělit na 3 typy:

- ☐ Technologické – měří výkonnost a dostupnost komponent infrastruktury a aplikací.
- ☐ Procesní – měří výkonnost procesů Service Managementu a jsou založeny na tzv. Key Performance Indicators (KPIs) a Critical Success Factors (CSFs). Jsou to kvantitativní či kvalitativní ukazatelé výkonnosti, kvality, hodnoty nebo dodržování procesů. Příkladem kvalitativního KPI je spokojenost zákazníka, zatímco kvantitativním ukazatelem můžou být náklady spojené s incidentem.
- ☐ Metriky služeb – jedná se o výsledky koncové služby a jsou měřeny s využitím metrik komponent.

3.5.2 Continual Service Improvement Process

Proces popisuje způsob provádění měření a vytváření reportů. Skládá se ze sedmi kroků, které zahrnují shromáždění dat, jejich analýzu, prezentaci výsledků managementu a implementaci zlepšovacích návrhů (viz Obr. 14). Každý krok je řízen strategickými a taktickými cíli, definovanými v Service Strategy a Service Design.

Definice toho, co by mělo být měřeno

Na počátku procesu CSI je vytvořen seznam aspektů, které by měly být měřeny. Definice je závislá především na požadavcích byznysu. Tento krok vychází z identifikace vize, strategie, taktických a operačních cílů organizace.

Definice toho, co může být měřeno

Na základě předchozího kroku, procesních toků, procedur a používaných nástrojů se zjistí, co všechno může být měřeno. Měřicí nástroje zahrnují nástroje pro správu služeb, monitorovací zařízení, nástroje pro tvorbu reportů, vyšetřování a další. V případě nedostatečných možností měření je nutné pořídit nové nástroje nebo přizpůsobit a nakonfigurovat nástroje tak, aby byly schopny měřit v plné míře to, co je požadováno.

Shromáždění dat

Pro samotný sběr dat je zapotřebí určitých monitorovacích nástrojů v podobě aplikací, systémů, nástrojů pro monitoring komponent aj. Klíčovým záměrem monitoringu v rámci CSI je dosažení kvality, zaměřuje se tedy na efektivitu služeb, procesů, nástrojů nebo CI.

Zpracování dat

Dalším krokem v procesu CSI je zpracování dat. Zpracování spočívá v tom, že shromážděná data jsou převedena do požadovaného formátu. Využívá se zde metoda generování zpráv, která je předmětem procesu Service Reporting. Zpracování dat je velice důležitá část procesu, protože nám mimo jiné umožňuje pochopit dopad jednotlivých komponent infrastruktury na ostatní komponenty a IT službu.

Analýza dat

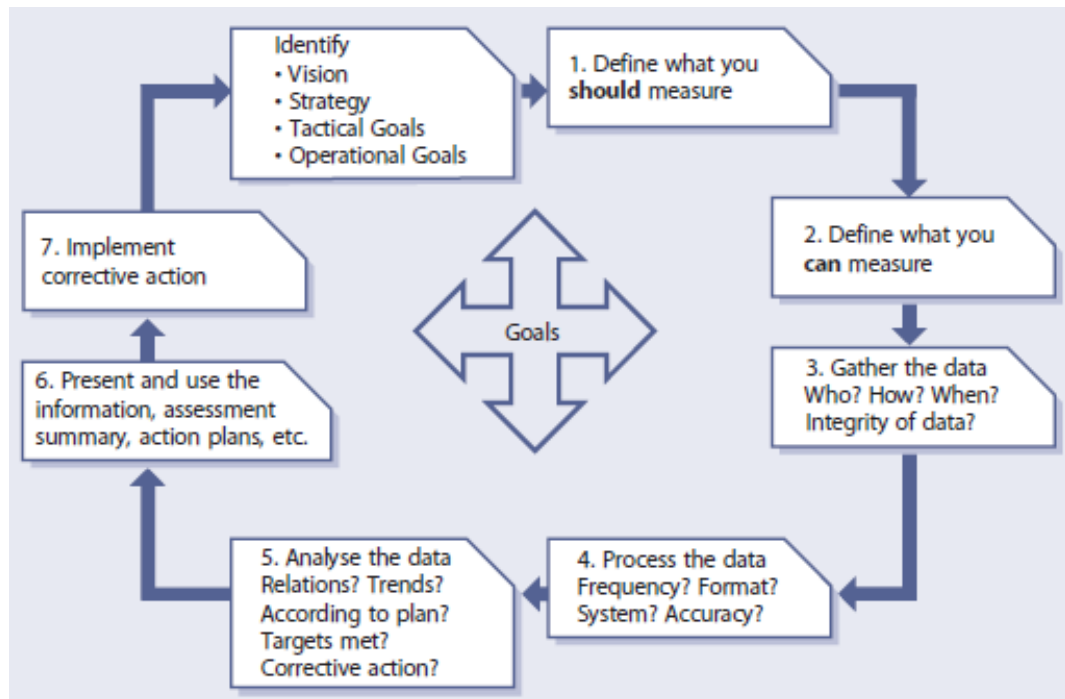
Na základě získaných informací a jejich analýzy jsme schopni odhalit události, které ovlivňují organizaci. Dojde k ověření cílů organizace a zjistí se, zda jsou potřebné nějaké nápravné kroky, popř. jaké budou jejich náklady.

Prezentace a použití informace

V této aktivitě jsou zjištěné informace prezentovány managementu ve srozumitelném formátu, na základě kterého je možno učinit strategická, taktická a operační rozhodnutí.

Implementace nápravné akce

Informace a znalosti získané v předchozích krocích jsou nyní využity k optimalizaci, vylepšení a nápravě služeb, procesů a všech dalších podpůrných aktivit a technologií. Po rozhodnutí o změně v rámci poskytované služby či procesu správy služeb pokračuje životní cyklus služby – definicí nové strategie (Service Strategy), návrhem změny ve službě (Service Design), nasazením změn do produkčního prostředí (Service Design) a správou každodenních operativních aktivit (Service Operation).



Obr. 14: Continual Service Improvement Process [13]

3.5.3 Service Reporting

Informační technologie zpracovávají a monitorují velké množství dat během dennodenního poskytování služeb, nicméně, jen některé z nich jsou pro byznys důležité. Reporty reprezentují historický přehled výkonnosti služby či procesů. Zaměřují se především na historické události, které mohou být potenciální hrozbou v budoucnu, a popisují, jak se organizace hodlá s těmito hrozbami vypořádat.

4 Formální zápis byznys procesů pomocí Petriho sítí

Zatímco neformální způsoby specifikace procesů obvykle využívají přirozeného jazyka, popřípadě dalších prostých prvků, jako jsou tabulky, obrázky a jednoduché diagramy, formální metody se vyznačují svou přesně definovanou sémantikou a syntaxí. Pomocí formálních metod jsme schopni specifikovat danou problematiku jednoznačně.

Petriho síť reprezentují jednu ze základních možností formalizace byznys procesů. Pomocí této metody, která vznikla jako rozšíření konečných automatů, je možno procesy jednoznačně popsat, modelovat a analyzovat.

4.1 Petriho síť

Stejně jako standardy UML, BPMN a EPC umožňují i Petriho síť (Petri Nets - PN) zápis byznys procesů pomocí grafické notace, která zahrnuje prvky symbolizující například souběžné vykonávání aktivit, varianty alternativních toků či provádění iterací. Nicméně, na rozdíl od zmíněných standardů se Petriho síť vyznačují přesnou matematickou definicí a rozvinutou matematickou teorií, která umožňuje jejich podrobnou analýzu.

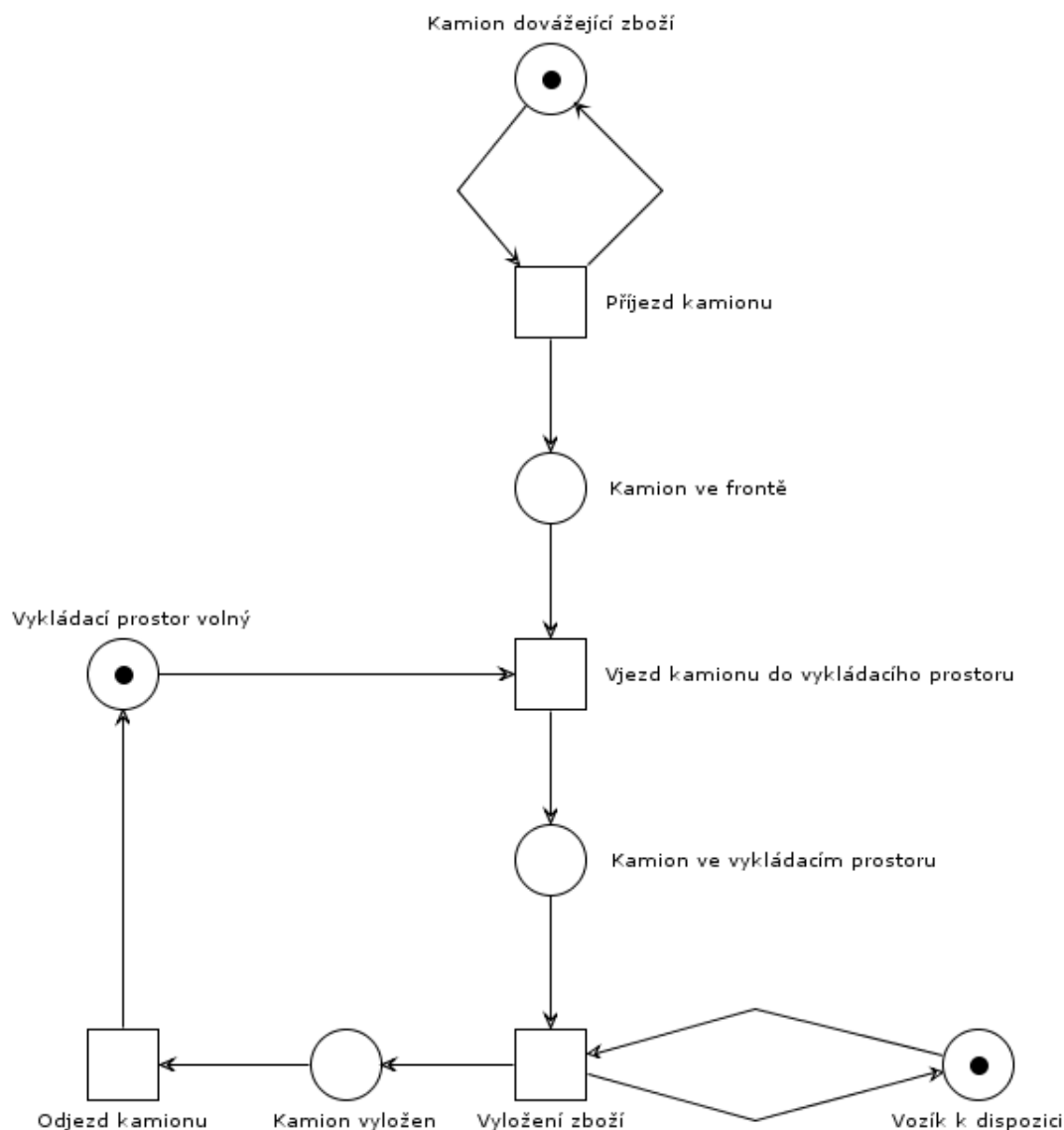
4.1.1 Klasické Petriho síť

Petriho síť modelují dynamické systémy prostřednictvím statické struktury. Statická struktura je reprezentována komponentami sítě. Komponentami mohou být místa (places), přechody (transitions) nebo orientované hrany (directed arcs) spojující místa s přechody. Místa jsou znázorněna kruhem a přechody čtvercem. Petriho síť představují bipartitní graf – to znamená, že žádná hrana přímo nespojuje dvě místa či dva přechody. Každému přechodu náleží množina vstupních a výstupních míst.

Dynamičnost formalizovaného systému je zajištěna pomocí tzv. tokenů, které jsou znázorněny černými tečkami uvnitř kruhů (míst). Počet tokenů v jednotlivých místech je dán označováním (marking), což je aktuální distribuce tokenů v síti. Tím je charakterizován stav modelovaného systému v určitém momentě. Provedení přechodu je možné pouze tehdy, pokud je proveditelný. Proveditelnost přechodu spočívá v tom, že se ve všech jeho vstupních místech vyskytuje alespoň jeden token (černá tečka). Jestliže je přechod proveden, je odebrán jeden token ze všech vstupních míst a do každého výstupního místa je jeden token přidán. V kontextu s podnikovými procesy přechody reprezentují aktivity procesu a místa odpovídají jeho stavům.

Problematika Petriho sítí je popsána v knize „Business Process Management“. [14]

Následující obrázek (viz Obr. 15) ilustruje příklad modelu jednoduchého procesu pravidelné vykládky zboží přivezeného kamionem do obchodu. Po příjezdu k obchodu je kamion nucen vyčkat ve frontě, dokud se neuvolní vykládací prostor. Jakmile je prostor volný, může do něj kamion najet. V případě, že je k dispozici vykládací vozík, je možno zboží vyložit a převést do skladu. Po vyložení zboží může kamion odjet z vykládacího prostoru a umožnit tak vjezd do prostoru jiným kamionům. Vykládací vozík je uvolněn pro další vykládku.



Obr. 15: Příklad modelování jednoduchého procesu pomocí Petriho sítí

4.1.2 Rozšíření klasických Petriho sítí

Klasické Petriho sítě byly aplikovány do mnoha praktických oblastí, jako například distribuované informační systémy, výrobní a průmyslové systémy, komunikační protokoly, aj. Řešení některých reálných problémů pomocí klasických Petriho sítí však může být poněkud obtížné, a proto je vhodné obohatit jejich modelovací možnosti o tzv. rozšíření. Jednou z oblastí, ve které se využívá rozšíření klasických PN, jsou tzv. workflow systémy – nástroje pro definici, automatizované řízení, monitorování a optimalizaci podnikových procesů. Sítě rozšířené o další vlastnosti nazýváme souhrnně Petriho sítě vyšší úrovně (High-level Petri Nets), které klasické PN rozšiřují například o barvu (reprezentující data), čas, nebo mohou poskytnout hierarchickou strukturalizaci pro modelování rozsáhlých sítí.

□ Rozšíření o barvy

V barevných Petriho sítích obvykle tokeny zastupují různé objekty, jako například prostředky, dokumenty, produkty nebo lidi. Barvu tokenu chápeme jako množinu určitých hodnotu objektu, která popisují jeho vlastnosti. Přechody pak produkují tokeny v závislosti na hodnotách tokenů v jejich vstupních místech. V rámci přechodů je možné specifikovat podmínky vyhodnocované před nebo po provedení přechodů (preconditions a postconditions), a tím je možné usměrňovat tok objektů v síti dle hodnot jejich atributů.

□ Rozšíření o čas

V reálných procesech nejsou prováděny jednotlivé přechody okamžitě za sebou, ale s určitým časovým zpožděním, které je dáno časem spotřebovaným během vykonávání aktivit. Časované sítě jsou tedy mechanismem Petriho sítí obohaceným o koncept času. Časové charakteristiky mohou být aplikovány na různé komponenty PN – přechody, místa, hrany či tokeny. Každá z těchto variant s sebou přináší jisté výhody a nevýhody. Nejpřirozenější možností je aplikace času na přechody, kdy doba přechodu přímo odpovídá trvání příslušné aktivity.

□ Hierarchické rozšíření

Jelikož mohou být skutečné procesy velmi složité a rozsáhlé, mohou být tyto procesy modelované prostřednictvím Petriho sítí strukturovány do menších celků. Tento problém řeší tzv. hierarchické Petriho sítě, které zavádí pojem podsít' (subnet), což je množina přechodů, míst, hran, popř. dalších podsítí. Procesy tak mohou být pro lepší přehlednost rozděleny na podprocesy, které popisují chování částí procesů ve větším detailu.

Možnosti rozšíření klasických PN jsou specifikovány v dokumentu „Modelling and analysing workflow using a Petri-net based approach“. [15]

4.2 Možnosti formálního zápisu procesů pomocí Petriho sítě

Tato diplomová práce se zabývá dvěma základními způsoby formálního zápisu byznys procesů pomocí Petriho sítě, kterými jsou workflow síť a metoda Business Process Modeling.

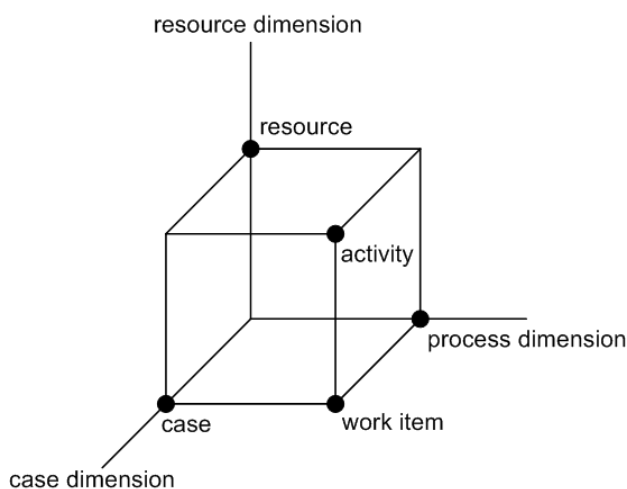
4.2.1 Workflow síť

Workflow síť vznikají mapováním workflow na Petriho síť. Následující podkapitoly popisují, co pojem workflow znamená, proč je vhodné mapovat workflow na Petriho síť a jaká jsou specifika této techniky.

4.2.1.1 Workflow

Pojmem workflow rozumíme abstraktní znázornění byznys procesů, tedy posloupnosti opakujících se činností v organizaci, které jsou vykonávány jistými osobami nebo skupinami osob, jejich zpracování a automatizované řízení prostřednictvím informačních technologií. Workflow staví na systematické organizaci prostředků, definici rolí a řízeném toku dat, informací či dokumentů. Mechanismus workflow je obvykle integrován do podnikových systémů, jako jsou ERP nebo CRM.

Koncept workflow můžeme znázornit pomocí tří dimenzí (viz Obr. 16) – dimenze procesní (process dimension), dimenze případová (case dimension) a dimenze zdrojů (resource dimension). Dimenze případů značí, že každý případ workflow je řešen individuálně. Každá činnost specifikovaná pomocí workflow je prováděna pro konkrétní případ, který je často vyvolán externím nebo interním zákazníkem organizace. V rámci případů jsou dle specifikovaných pravidel vykonávány jednotlivé úlohy (tasks). Jedna úloha může být prováděna mnoha případy, úlohu v kontextu s konkrétním případem nazýváme pracovní položkou (work item). Pro realizaci pracovních položek je většinou zapotřebí určitých zdrojů (resources). Zdrojem může být zařízení (např. tiskárna) nebo osoba (např. zaměstnanec). Pro snadnější přidělování pracovních položek zdrojům jsou zdroje seskupovány do tříd (resource classes). Jestliže je klasifikace zdrojů založena na organizační struktuře, nazýváme takovéto třídy organizačními jednotkami (organizational units). V případě, že jsou jednotlivé zdroje seskupovány dle jejich schopností, nazýváme třídy rolemi (roles). Pracovní položka, která je prováděna prostřednictvím určitých zdrojů, je reprezentována aktivitou (activity).



Obr. 16: Tři dimenze konceptu workflow

Koordinace mezi aktivitami a účastníky procesu je zpravidla řízena informačním systémem, který se nazývá Workflow Management System (WfMS). WfMS zajišťuje, že ve správný okamžik je příslušným zdrojům (osoby nebo systémy) adresována náležitá činnost. Jakmile je určitá aktivita v rámci procesu dokončena, WfMS rozhodne na základě definice workflow o tom, jak bude provádění procesu pokračovat. Definice workflow je reprezentována modelem byznys procesu, který popisuje tok činností a jejich vzájemné závislosti. Definice rovněž obsahuje informace o prostředcích nezbytných pro vykonání konkrétní aktivity.

Díky efektivnímu řízení toku informací v procesech dochází k výraznému snížení nákladů, vyšší efektivitě procesů, zkvalitnění poskytovaných služeb a tím také ke zvýšení konkurenceschopnosti podniku.

Koncept workflow je popsán v dokumentu „The Application of Petri Nets to Workflow Management“. [16]

4.2.1.2 Důvody mapování workflow na Petriho síť

V rámci workflow systémů rozlišujeme modelování dvou aspektů organizace – podnikových procesů a zdrojů. Většinou jsou tyto dva aspekty specifikovány odděleně a to z několika důvodů – možnost modifikace procesů bez zásahu do organizačního modelu, větší pravděpodobnost opětovného použití a rovněž snížení složitosti jednotlivých modelů.

Pro formální popis procesní dimenze workflow je vhodné využít metodiky Petriho sítí. Přizpůsobením Petriho sítí workflow modelům vznikají tzv. workflow síť (Workflow Nets – WF-nets), pomocí kterých lze precizně popsat i komplexní byznys procesy.

Díky formální sémantice procesů, které jsou specifikovány Petriho sítěmi, je možné také analyzovat vlastnosti jednotlivých procesů. Například mohou být procesy verifikovány – tzn. ověřeny, zda neobsahují logické chyby (například tzv. deadlock či livelock), nebo validovány – tzn. potvrzeny, že popisují skutečnou situaci. Validace ovšem vyžaduje adekvátní znalost daných podnikových procesů. Další možností rozboru procesů je tzv. výkonnostní analýza, která například prostřednictvím simulace procesu ověřuje, zda byly splněny požadavky procesu s ohledem na čas a zužitkované prostředky. Pro validaci, verifikaci a výkonnostní analýzu workflow procesů byla vyvinuta celá řada technik.

Další výhodou využití Petriho sítí pro modelování byznys procesů je explicitní modelování stavů jednotlivých případů (state-based). Tím se odlišují od modelovacích technik založených na událostech (event-based), pomocí kterých jsou modelovány explicitně přechody a implicitně stavy. Techniky založené na stavech umožňují rozlišit aktivaci úlohy (enabled) od jejího vykonávání. Vykonávání je započato až ve chvíli, kdy je vyvolán spouštěč (tzv. trigger). Díky technikám založeným na stavech je možno také lépe modelovat souběžné úlohy. Dvě úlohy jsou souběžnými, pokud jsou obě aktivovány a je možno provést pouze jednu z nich. [17]

4.2.1.3 Popis Workflow sítí

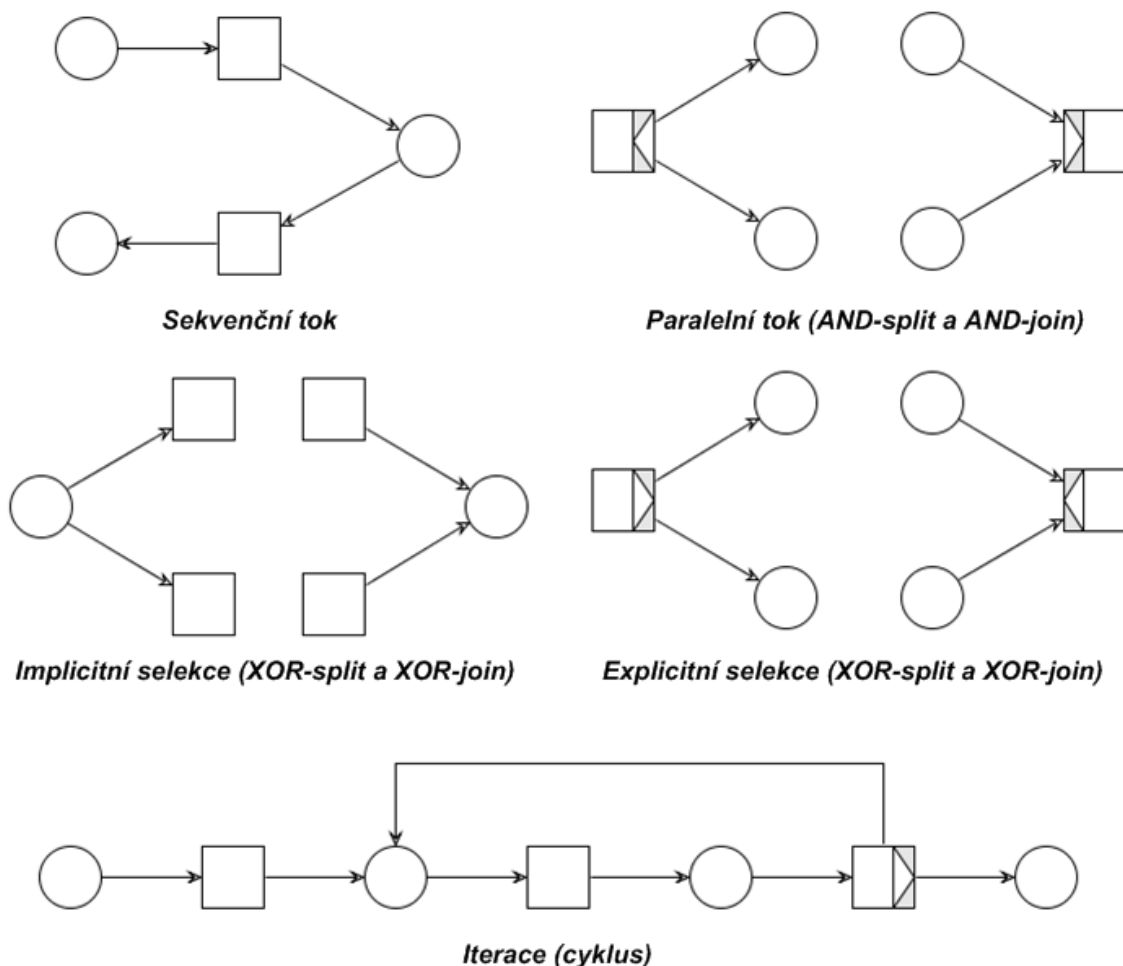
Každá workflow síť definuje jedno vstupní místo (i) a jedno výstupní místo (o). Token ve vstupním místě sítě značí počátek provádění konkrétního případu, zatímco token ve výstupním místě signalizuje, že daný případ procesu byl již vykonán. V rámci workflow sítí musí platit, že každý přechod (úloha) či místo (podmínka) se podílí na vykonávání určitého případu (instance procesu). To znamená, že každý přechod nebo místo se nachází na cestě ze vstupního do výstupního místa. Pokud je splněn požadavek, že pro každou libovolnou dvojici přechodů (či

míst) existuje cesta vedoucí z jednoho přechodu do druhého, říkáme, že síť je silně propojená (strongly connected). Tohoto požadavku může být docíleno přidáním dalšího přechodu, který propojuje výstupní místo se vstupním.

Pro odlišení instancí procesu se využívá Petriho sítě vyšší úrovně, konkrétně barevných Petriho sítí, ve kterých hodnota tokenů reprezentuje danou instanci. Alternativní možností zpracování více instancí procesu je vytvoření samostatných kopií příslušné Petriho sítě pro každý speciální případ.

Konstrukce používané pro směřování tokenů v síti

Při modelování procesů pomocí workflow sítí je možno využít několika vzorů stavebních bloků pro směřování tokenů v síti v závislosti na logice vykonávání aktivit procesu (viz Obr. 17). Konstrukce zahrnují stavební bloky pro sekvenční, paralelní, podmíněné vykonávání aktivit a rovněž vzor pro zakomponování cyklu do sítě – iterace.



Obr. 17: Řídící konstrukce workflow sítí

Spouštěče

Je nutné zmínit, že pokud je daná úloha aktivovaná pro daný případ, nemusí to ještě znamenat, že bude úloha bezprostředně provedena. Provedení úlohy není možné workflow systémem vynutit. Je proto důležité rozlišovat mezi aktivací (enabled) a vykonáním (execution) úlohy.

Spouštěč (trigger) je externí podmínkou, která vede k provedení konkrétní aktivované úlohy. Vykonání instance úlohy začíná v okamžiku, kdy je instance spuštěna – tzn., když je externí podmínka splněna. Spouštěče můžeme rozdělit na několik typů (viz Obr. 18):

☐ Automatický (automatic)

Tento typ je aplikován na úlohy prováděné aplikacemi bez nutnosti zásahu osob. Úlohy jsou spuštěny bezprostředně po jejich aktivaci.

☐ Uživatel (user)

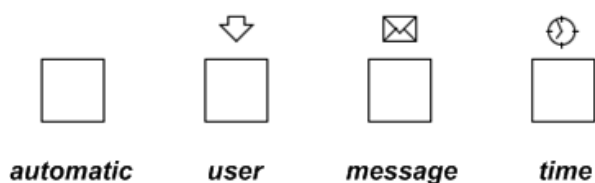
Úlohy typu uživatel jsou spouštěny člověkem – účastníkem procesu.

☐ Zpráva (message)

U tohoto typu je spouštěč reprezentován určitou zprávou, jako například e-mail, faxová zpráva, telefonní hovor, apod.

☐ Čas (time)

V tomto případě je spouštěčem čas, který je předem nadefinovaný. Například je možno nadefinovat, že má být určitý dokument uložen do archivu, pokud nebyl modifikován určitý počet hodin.



Obr. 18: Typy spouštěčů úloh ve workflow sítích (triggers)

4.2.1.4 Korektnost workflow sítě

Základním a velice důležitým požadavkem organizace je korektnost byznys procesů specifikovaných v systémech workflow. Samozřejmostí pro definici korektní sítě je splnění dvou podmínek, které byly zmíněny v popisu workflow sítě – tedy existence jednoho vstupního, jednoho výstupního místa a zajištění, že každý přechod či stav se nachází na cestě z místa vstupního do místa výstupního.

Nieméně, tyto podmínky nezaručují eliminaci potenciálních chyb jako je deadlock nebo livelock. Deadlock je situací, kdy dojde k zablokování procesu v určitém stavu z důvodu neproveditelnosti žádného z následujících přechodů. Livelock znamená uvíznutí v nekonečném cyklu, který není možné opustit.

Korektní síť musí vyhovovat následujícím dvěma podmínkám, popisujícím vlastnost workflow sítě, kterou nazýváme spolehlivost (soundness). První podmínkou spolehlivé sítě je,

že každý případ workflow (instance procesu) musí být kompletně ukončen. To znamená, že v okamžiku, kdy je proces ukončen, se nachází ve výstupním místě tolik tokenů, kolik jich bylo na počátku procesu ve vstupním místě, a ostatní místa jsou prázdná. Neexistuje tedy žádná aktivita procesu, která by byla aktivní po ukončení procesu. Druhým předpokladem spolehlivosti je, že workflow síť neobsahuje žádné nadbytečné aktivity. Jinými slovy, všechny přechody musí být dosažitelné ze vstupního místa a zároveň ze všech přechodů musí být dosažitelné výstupní místo. K ověření spolehlivosti definovaných workflow sítí je možno využít různých metod, příkladem je tzv. graf dosažitelnosti.

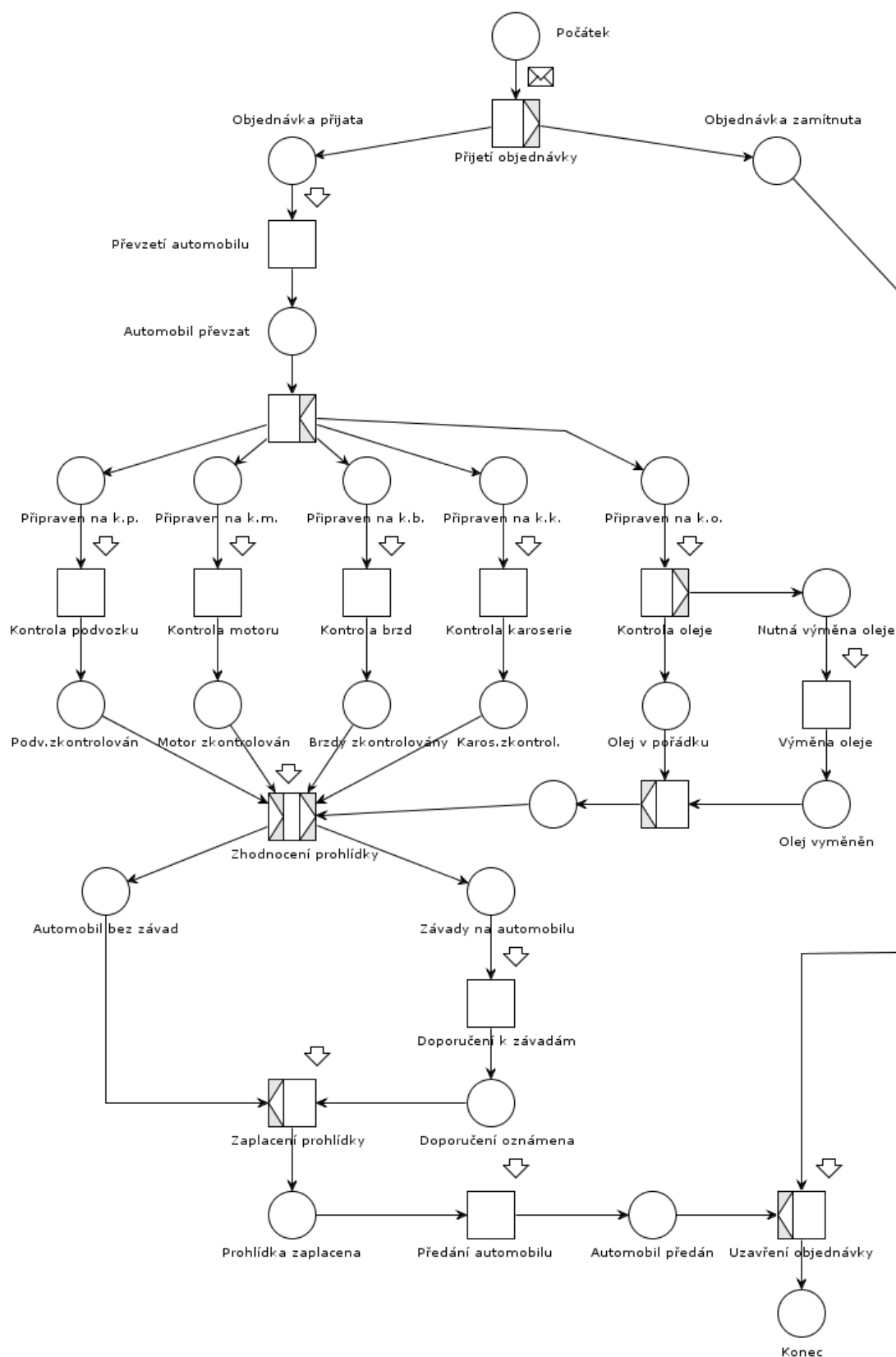
Problematika workflow sítí je popsána v dokumentu „The Application of Petri Nets to Workflow Management“ [16] a publikacích „Lectures on concurrency and Petri nets: advances in Petri nets“ [18] a „Metody byznys modelování“ [19].

4.2.1.5 Ukázka modelování jednoduchého procesu pomocí workflow sítí

Pro názornou ukázkou modelování procesů pomocí workflow sítí byl vybrán proces, který popisuje zjednodušenou servisní prohlídku automobilů (viz Obr. 19).

Proces je zahájen přijetím objednávky od zákazníka, kterou může zaměstnanec servisního oddělení přijmout nebo zamítnout. Spouštěčem této aktivity je tedy zpráva (message), která může nabývat různého charakteru – telefonní hovor, elektronická objednávka, email, aj. Pokud byla objednávka zamítnuta, dojde k jejímu uzavření a proces je u konce. V případě přijetí objednávky je v rámci aktivity „Přijetí objednávky“ domluven se zákazníkem termín konání servisní prohlídky. Ve smlouvenou dobu pak dojde k převzetí automobilu zaměstnancem servisu. Zákazník předá příslušnému zaměstnanci všechny potřebné náležitosti (klíče, servisní knihu, apod.) a obdrží doklad o převzetí automobilu servisem. Po převzetí je automobil připraven k servisní prohlídce. Prohlídka zahrnuje kontrolu podvozku, karoserie, motoru, brzd a rovněž motorového oleje. V rámci kontroly oleje servisní technik rozhodne, zda je vhodná doba pro kompletní výměnu oleje. Pokud je výměna oleje nezbytná, je servisní technik povinen výměnu provést. Na závěr prohlídky jsou všechny úkony zhodnoceny, jsou sepsány případné připomínky a nalezené závady. V případě zjištění závad na automobilu je zákazníkovi předáno doporučení pro jejich odstranění. Po zaplacení prohlídky je zaměstnanec servisu odpovědný za předání automobilu a všech náležitostí zákazníkovi. Následně může být objednávka formálně uzavřena.

V ukázkovém modelu procesu platí obě podmínky charakterizující spolehlivé workflow síť. Každý případ je řádně ukončen – žádný přechod tedy nezůstane aktivní po ukončení procesu. Zároveň se v této síti nenacházejí žádné přebytečné aktivity. Workflow síť je možno označit za spolehlivou.



Obr. 19: Ukázka modelování jednoduchého procesu pomocí workflow sítí

4.2.2 Business Process Modeling

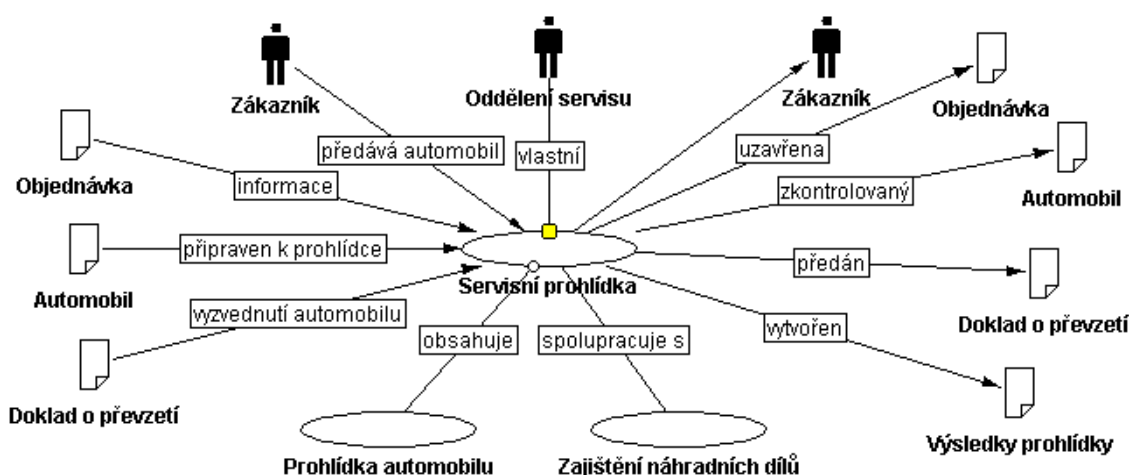
Business Process Modeling (BPM) je další metodou, která umožňuje byznys procesy nejen popsat, ale rovněž simulovat, analyzovat a řídit. BPM umožňuje analyzovat strukturální vlastnosti procesů, následně simulovat jejich průběh a zároveň měřit jejich kvantitativní charakteristiky, jako např. čas nebo náklady. Tato metoda přináší organizaci značnou míru flexibility v rámci návrhu byznys procesů, jelikož umožňuje snadnou modifikaci ve specifikaci procesu, okamžité ověření nového návrhu procesu a jeho rychlé znovupoužití.

Každý byznys proces specifikovaný pomocí metody BPM je zachycen třemi odlišnými modely, které popisují proces z různých úhlů pohledu. V následujících podkapitolách jsou vysvětlena základní specifika jednotlivých modelů a jejich notace.

4.2.2.1 Funkční model (Functional Model)

Funkční model je základním modelem poskytujícím obecný přehled nad procesy používanými v organizaci a jejich strukturou, a znázorňuje všechny vstupy a výstupy jednotlivých procesů. Struktura procesů může být zachycena prostřednictvím dvou typů vazeb – podproces (containment) a spolupráce (collaboration). Proces je ve vztahu s podprocesem, jestliže spouští příslušný podproces se záměrem získání požadovaných výstupů. Podproces mohou využívat různé procesy. Spolupráce definuje možný souběh dvou či více procesů. Model rovněž popisuje jednotlivé zákazníky a produkty.

Na obrázku (viz Obr. 20) je vidět příklad funkčního modelu procesu „Servisní prohlídka“. Na levé straně modelu se nacházejí všechny objekty vstupující do procesu – tj. „Zákazník“, „Objednávka“, „Automobil“, „Doklad o převzetí“. Na pravé straně obrázku jsou pak zaznačeny objekty vystupující z procesu. Vstupující objekty jsou tedy spojeny s procesem hranou orientovanou směrem do procesu, naopak vystupující objekty jsou propojeny s procesem hranou orientovanou k daným objektům. Hrana může být také rozšířena o krátký popis, který specifikuje stav nebo význam objektu. V modelu je také patrná notace pro vlastníka procesu (vazba „vlastní“), obsažený podproces (vazba „obsahuje“) a spolupracující proces (vazba „spolupracuje s“).

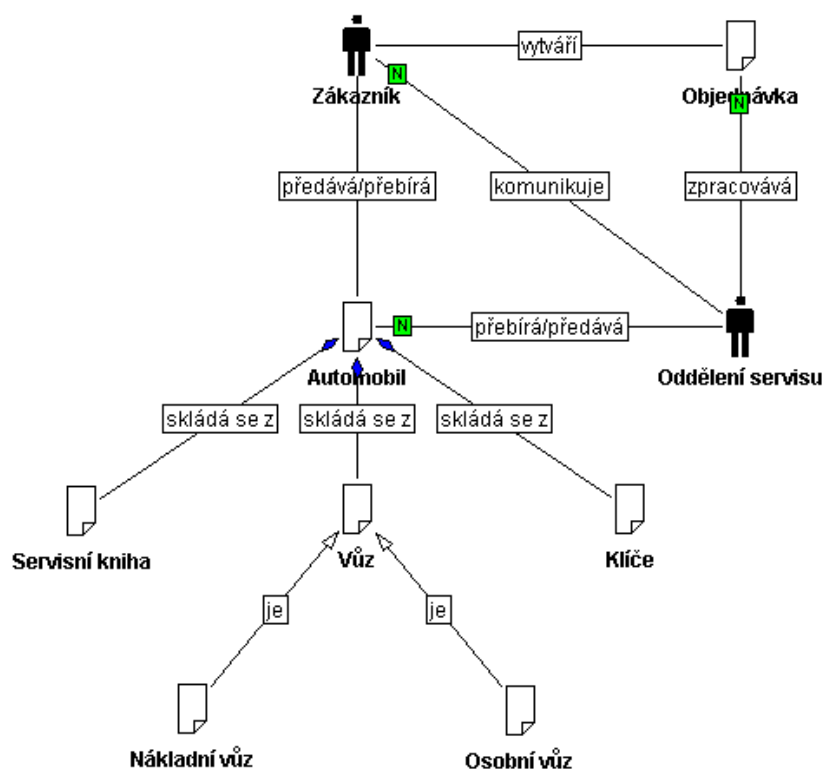


Obr. 20: Příklad funkčního modelu metody BPM

4.2.2.2 Objektový model (Object Model)

Tento model zachycuje statickou strukturu a souvislosti všech objektů (entit), které se procesu účastní. Všechny entity mohou být popsány množinou atributů. Jsou zde specifikovány aktivní objekty, které mají za úkol vykonávání aktivit, a pasivní objekty, se kterými proces zachází, jako například dokumenty, produkty, apod.

Ukázkový příklad objektového modelu BPM (viz Obr. 21) se zaměřuje rovněž na popis procesu „Servisní prohlídka“. Nicméně, v tomto případě je zachycena struktura některých aktivních a pasivních objektů vyskytujících se v procesu. Proces zahrnuje dva aktivní objekty – „Zákazník“ a „Oddělení servisu“. Aktivní objekty manipulují v průběhu jednotlivých aktivit s objekty pasivními (např. „Oddělení servisu“ zpracovává „Objednávku“), popřípadě jsou v přímé interakci s dalšími aktivními objekty (např. „Oddělení servisu“ komunikuje se „Zákazníkem“). Tomuto typu vazby říkáme asociace. Další důležitou vazbou mezi dvěma aktivními nebo pasivními objekty, která nese atribut „skládá se z“, je kompozice. V ukázkovém modelu tato vazba sděluje, že objekt „Automobil“ zahrnuje nejen samotné vozidlo, ale také další náležitosti, které musí „Zákazník“ v servise zanechat při předávání vozu – tj. „Servisní kniha“ a „Klíče“. Další vazbou, která propojuje dva aktivní či dva pasivní objekty, je zobecnění (označení „je“). „Osobní vůz“ a „Nákladní vůz“ jsou speciálními případy objektu „Vůz“. Ten je naopak jejich zobecněním. Vazby v objektovém modelu lze rovněž doplnit o násobnosti.



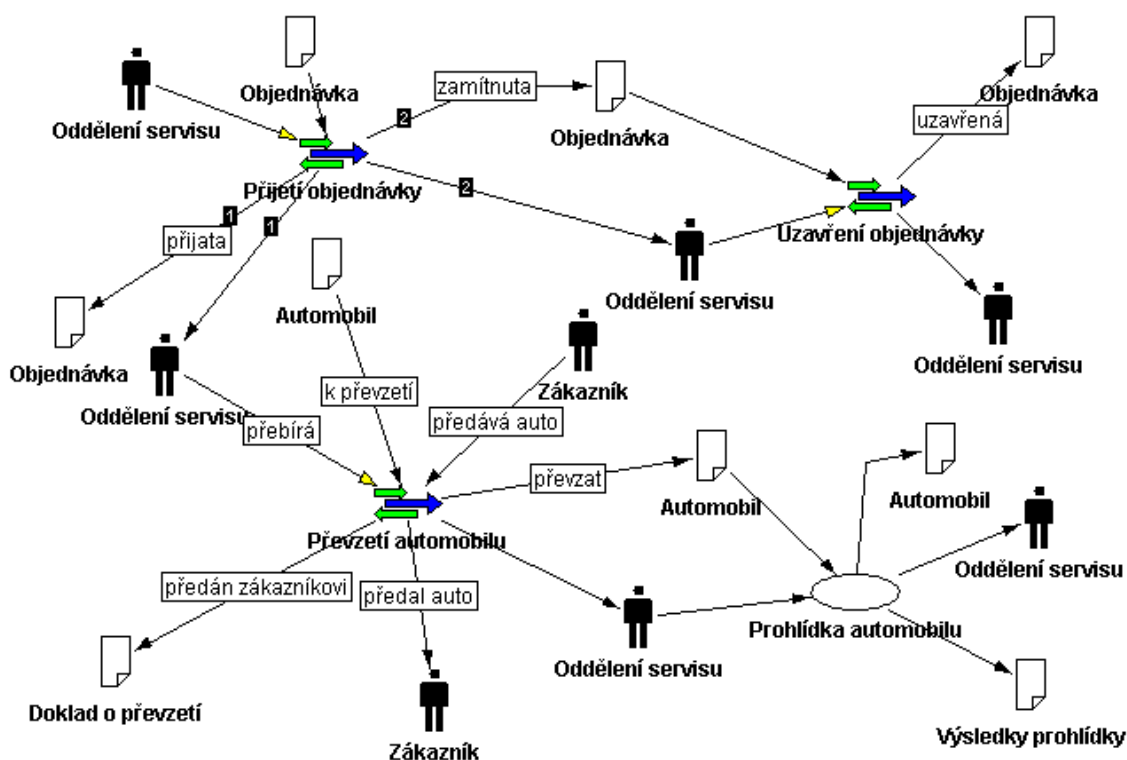
Obr. 21: Příklad objektového modelu metody BPM

4.2.2.3 Koordinační model (Coordination Model)

Nejdůležitějším modelem je tzv. koordinační model, který je založen na principu Petriho sítí. Tímto modelem je popsána posloupnost jednotlivých aktivit, jsou specifikovány podmínky

usměrňující tok objektů v procesu, rovněž je zachycena interakce mezi aktivními a pasivními objekty, a je definována jejich účast v aktivitách. V rámci posloupnosti aktivit jsou zahrnuty i případné podprocesy, specifikované ve funkčním modelu.

Následující obrázek (viz Obr. 22) znázorňuje principy a prvky notace používané v koordinačním modelu BPM. Na obrázku, který z důvodu přehlednosti pokrývá jen část výsledného koordinačního modelu procesu „Servisní prohlídka“, jsou vidět tři aktivity: „Přijetí objednávky“, „Převzetí automobilu“ a „Uzavření objednávky“. Proveditelnost libovolné aktivity spočívá na přítomnosti jejích vstupujících objektů. Objekty vystupující z aktivity mohou být konečným výstupem procesu nebo mohou opět vstupovat do jiné aktivity, popř. podprocesu. Aktivita může být rozdělena na několik scénářů (viz aktivita „Přijetí objednávky“). Další tok objektů tedy spočívá ve výběru určitého scénáře dle podmínek specifikovaných v rámci aktivity. Čísla scénářů jsou zaznamenána pomocí speciálního atributu dané vystupující hrany. Dalším atributem hrany může být popis vypovídající o stavu objektu před či po vykonání aktivity. Za všechny uvedené aktivity je odpovědný aktivní objekt „Oddělení servisu“, což je vyznačeno orientovanou hranou se žlutou šipkou směřující ze zmíněného objektu do příslušné aktivity. Součástí tohoto úseku procesu je také podproces „Prohlídka automobilu“, který by v samostatném koordinačním modelu popisoval všechny činnosti, které prohlídka zahrnuje.



Obr. 22: Příklad koordinačního modelu metody BPM

Cílem uvedených demonstračních příkladů není kompletní formalizace úplného procesu, ale pouze objasnění základních principů, na kterých je technika BPM založena.

Metoda BPM je popsána v manuálu BP Studia. [20]

5 Formalizace základních procesů ITIL v3 metodou BPM

Tato kapitola demonstruje použití metody BPM pro formalizaci procesů rámce ITIL v3. Je nutné zmínit, že formalizace, která je součástí této diplomové práce, vychází pouze z obecného popisu procesů, který nalezneme v oficiálních publikacích rámce. Tato specifikace ovšem nereprezentuje jediný univerzální a všeobecně používaný model procesu, který by stačilo v libovolné organizaci jednoduše nasadit. V rámci formalizace byznys procesů musí být jednotlivé modely přizpůsobeny kultuře, zvykům a dalším specifickým potřebám daného podniku.

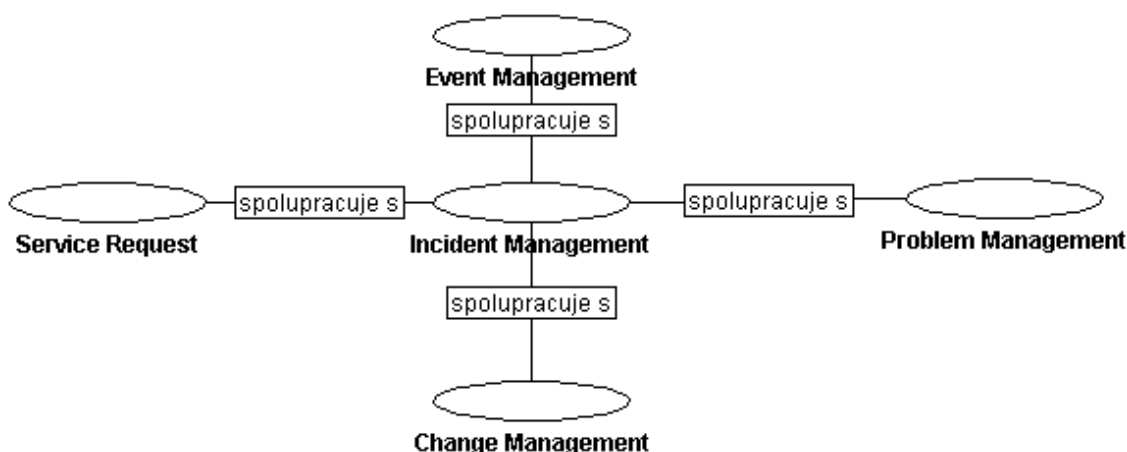
Pro formalizaci byly vybrány dva důležité procesy fáze operativní (Service Operation) – Incident Management a Problem Management, a také proces náležící do fáze přechodu IT služby (Service Transition) – Change Management. V této kapitole je možno shlédnout ukázkové modely procesu Incident Management, modely ostatních procesů včetně příslušných podprocesů se nacházejí v přílohách diplomové práce.

5.1 Ukázkové modely procesu Incident Management

Formalizace libovolného procesu pomocí metody BPM sestává z vytvoření tří základních modelů (viz kapitola 4.2.2).

5.1.1 Funkční model

Funkční model poskytuje obecný pohled na proces Incident Management. Pro snadnější pochopení a větší přehlednost byl vytvořen pro každý modelovaný proces specifický funkční model, který se zaměřuje pouze na kooperaci s ostatními procesy. Další aspekty funkčních modelů jsou detailněji rozpracovány v samostatném funkčním modelu. Kooperace procesu Incident Management je znázorněna na následujícím obrázku (viz Obr. 23).

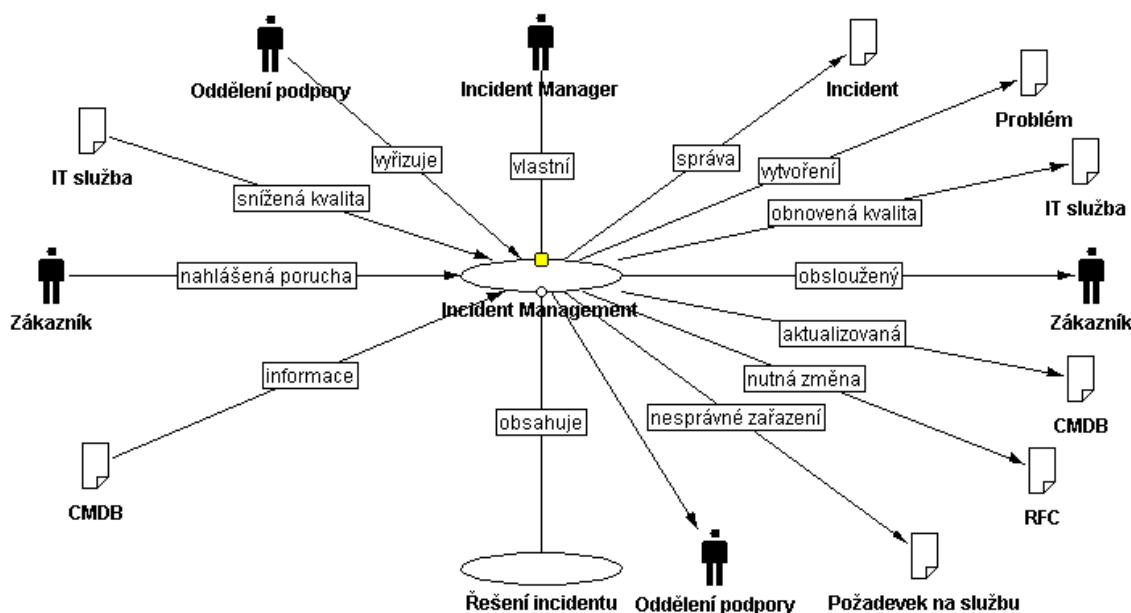


Obr. 23: Funkční model procesu Incident Management - spolupráce s ostatními procesy

Druhý funkční model (viz Obr. 24) znázorňuje všechny vstupy a výstupy procesu Incident Management, jeho vlastníka a obsažený podproces „Řešení incidentu“, který je poté rozpracován do podrobnějších detailů. Vstupem do procesu jsou aktivní objekty „Zákazník“ a „Oddělení podpory“. Zákazník hlásí poruchu nebo určité snížení kvality služby, zatímco „Oddělení podpory“ vyřizuje daný incident a je zodpovědné za učinění dalších kroků pro rychlé

obnovení smluvené kvality služby. Dalšími vstupy jsou pasivní objekty „IT služba“ se sníženou kvalitou a „CMDB“. Předpokládá se, že kromě popisu infrastruktury obsahuje databáze CMDB i informace o incidentech, problémech, známých chybách, požadavcích na změny (RFC), apod.

Všechny zmíněné vstupy jsou zároveň i výstupy procesu. Za jistých okolností může dojít během procesu k vytvoření dalších výstupů, jako je „RFC“, „Problém“ či „Požadavek na službu“. Tyto okolnosti jsou popsány v rámci koordinačního modelu. Vlastníkem procesu je „Incident Manager“, jehož odpovědností je sledovat efektivitu procesu a vytvářet doporučení pro jeho vylepšení, řídit práci podpory první a druhé úrovně, apod.

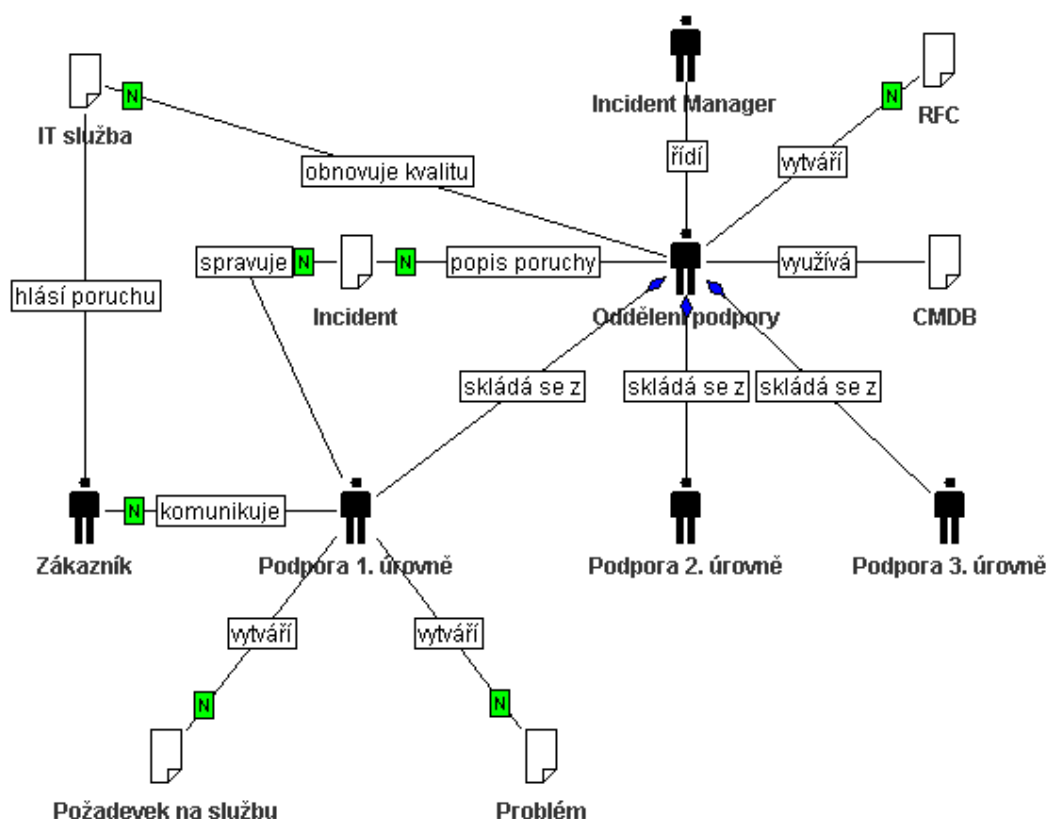


Obr. 24: Funkční model procesu Incident Management – vstupy, výstupy, aj.

5.1.2 Objektový model

Dalším modelem metody BPM, který popisuje byznys proces z jiného úhlu pohledu, je model objektový. Objektový model zachycuje všechny aktivní i pasivní objekty vyskytující se v procesu Incident Management, jejich vzájemnou souvislost a vztahy.

Na obrázku (viz Obr. 25) je možno vidět, že „Oddělení podpory“ je tvořeno třemi úrovněmi podpory, kde každá z těchto skupin pracovníků se může podílet na řešení incidentu a obnovování kvality „IT služby“, ale pouze „Podpora 1. Úrovně“ (Service Desk) obvykle reprezentuje přímý komunikační kanál mezi zákazníkem a organizací poskytující danou IT službu. Z obrázku je také patrné, že „Problém“ a „Požadavek na službu“ většinou vytváří pouze zaměstnanci „Podpory 1. úrovně“, zatímco požadavek na změnu „RFC“ může vytvořit kterákoliv úroveň z „Oddělení podpory“.



Obr. 25: Objektový model procesu Incident Management

5.1.3 Koordinační model

Nejdůležitějším modelem, popisujícím proces Incident Management pomocí metody BPM, je tzv. koordinační model (viz Obr. 26). Ten se zaměřuje na posloupnost aktivit, které jsou součástí procesu, znázorňuje odpovědnosti za jednotlivé aktivity, popisuje tok pasivních a aktivních objektů z jedné aktivity do druhé, a zobrazuje případnou změnu stavu objektů po vykonání aktivity.

Proces Incident Management může být nastartován ohlášením snížené kvality IT služby zákazníkem nebo prostřednictvím procesu Event Management. První aktivita procesu spočívá v záznamu detailů příslušného incidentu, které zahrnují podrobný popis symptomů. Jsou rovněž zkoumány podobné incidenty, které již byly zaevidovány v systému, a jsou popsány konfigurační položky, ke kterým se incident vztahuje.

Poté je ověřeno, zda se opravdu jedná o incident či pouze požadavek na službu. V prvním případě je incident zařazen do kategorie dle jeho charakteru, v druhém případě je vyvolán tzv. „Požadavek na službu“ a iniciativy se ujímá proces „Service Request“, který je určen právě ke správě požadavků. Z aktivity „Kategorizace incidentu“ tedy vychází aktualizovaný záznam incidentu. Následujícím krokem v procesu je stanovení priority incidentu dle jeho naléhavosti a dopadu na byznys. Také z této aktivity vychází záznam incidentu doplněný o náležitě informace.

Další aktivitou je tzv. „Počáteční diagnóza“, při které „Podpora 1. úrovně“ diagnostikuje incident a pokusí se nalézt adekvátní řešení, které by umožnilo rychlé zotavení služby. Popis

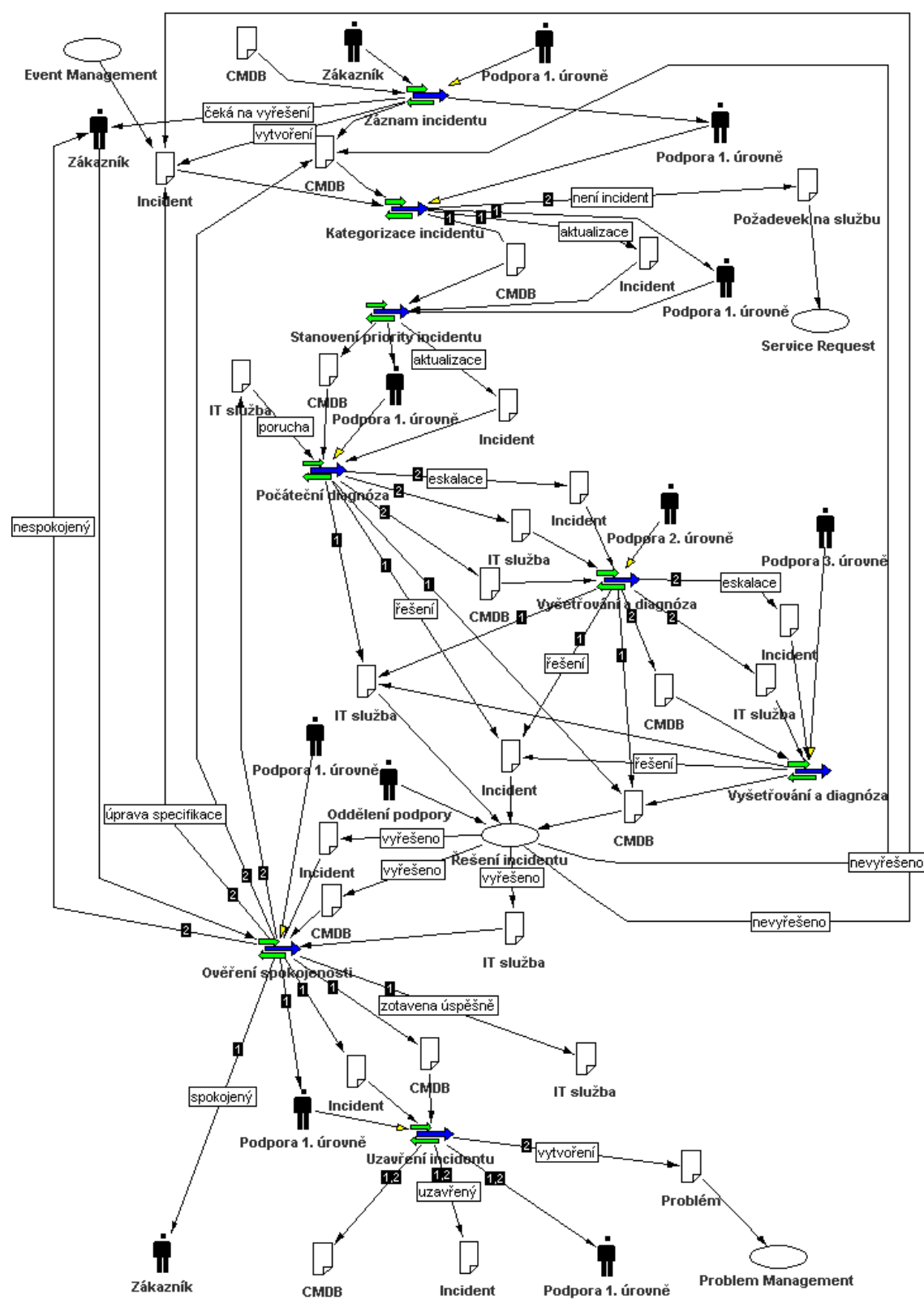
dočasného nebo úplného řešení se již může nacházet v databázi „CMDB“ z dříve analyzovaných a vyřešených incidentů. Pokud si „Podpora 1. úrovně“ s incidentem neví rady, je incident předán (eskalace) k diagnostice skupině pracovníků s většími technickými dovednostmi – „Podpora 2. úrovně“. Ta opět incident vyšetřuje a snaží se nalézt vhodné řešení. V případě, že ani tato skupina pracovníků není schopna navrhnout adekvátní řešení, je incident předán skupině specialistů zahrnující často dodavatele externích služeb, výrobce hardwaru, popř. i pracovníky procesu Problem Management – tj. „Podpora 3. úrovně“.

Po nalezení adekvátního řešení pokračuje proces aplikací daného řešení. Vyřešením incidentu se zabývá podproces „Řešení incidentu“, který je podrobněji popsán pomocí samostatného modelu.

Jakmile je incident vyřešen, jsou zaměstnanci podpory 1. úrovně odpovědni ověřit spokojenost zákazníka s řešením. Jestliže zákazník není s výsledkem spokojený, dojde k úpravě specifikace incidentu a v podstatě celý proces se opakuje. V opačném případě může být incident formálně uzavřen. V rámci uzavření je ověřeno, zda jsou veškeré náležitosti incidentu řádně dokumentovány a je přezkoumáno, zda byl incident správně klasifikován.

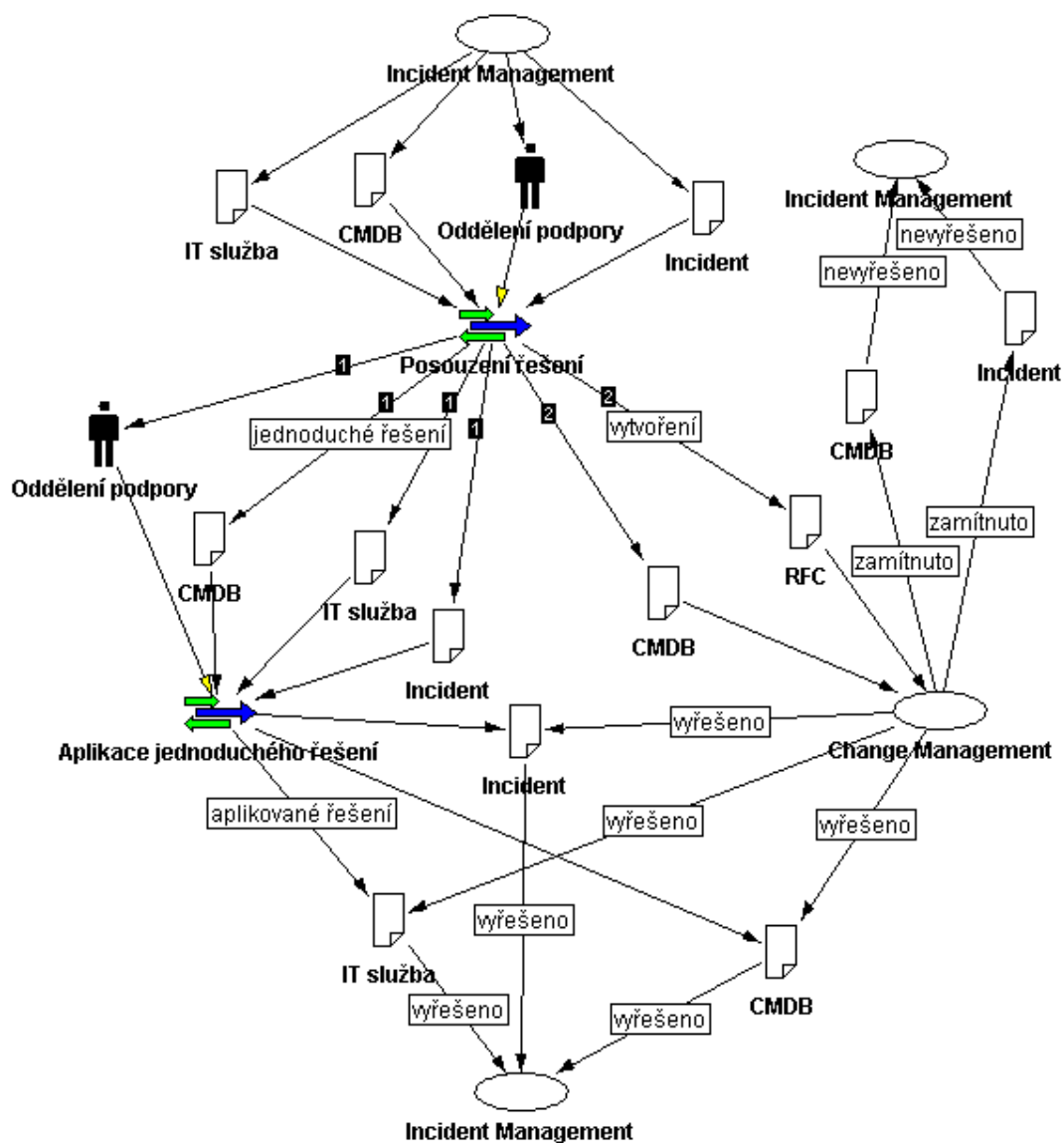
Na závěr rovněž dojde k rozhodnutí, zda je nutné vytvořit tzv. „Problém“ pro odhalení příčiny incidentu prostřednictvím procesu Problem Management. Vyvolání problému může být zpravidla následkem opakujících se incidentů, aplikace dočasného řešení incidentu (workaround) nebo výskytu incidentu s velkým dopadem (major incident).

Proces Incident Management, jeho aktivity a souvislosti s ostatními procesy, jsou detailněji popsány zejména v kapitolách 3.4.2 a 3.4.3.2.



Obr. 26: Koordinální model procesu Incident Management

Následující diagram (viz Obr. 27) reprezentuje koordinační model podprocesu „Řešení incidentu“, který znázorňuje dvě možnosti řešení incidentu. První možností je „Aplikace jednoduchého řešení“, kterým může být například restart serveru nebo síťového zařízení. Takovéto řešení nevyžaduje žádnou změnu ve službě, a proto může být zajištěno procesem Incident Management. Druhá možnost vyžaduje vytvoření „RFC“ a spolupráci s procesem Change Management, který je odpovědný za správu změn.



Obr. 27: Koordinační model podprocesu „Řešení incidentu“

Ostatní modely tohoto podprocesu se rovněž nachází v přílohách diplomové práce.

6 Závěr

V této diplomové práci jsem se seznámil se základními charakteristickými rysy, principy, procesy a dalšími důležitými vlastnostmi rámce ITIL v3, který je v dnešní době celosvětově uznávaným přístupem v oblasti ITSM a na jehož základech je postavena správa IT služeb mnoha významných organizací. Díky profesionálnímu a praxí ověřenému přístupu k řízení IT služeb přináší obvykle zavedení tohoto standardu v organizaci značné výhody, jako je například lepší kvalita a vyšší spolehlivost IT služeb, menší počet výpadků IT služeb, větší spokojenost zákazníků, efektivnější využívání drahých ICT zdrojů či úspora nákladů na provoz IT služeb. Práce je zaměřena především na ty záležitosti rámce, které staví na širokých znalostech informačních a komunikačních technologií a jejich řízení, naopak menší důraz byl kladen na otázky týkající se byznysu.

V další části diplomové práce jsem popsal metody formálního zápisu procesů založené na technice Petriho sítí. Díky využití techniky Petriho sítí je pomocí těchto metod možné nejen vytvořit modely byznys procesů, ale případně také ověřit jejich korektnost, či provést výkonnostní analýzu těchto modelů.

Výsledkem mé práce je také formální popis některých významných procesů ITIL v3 pomocí metody BPM. Je nutné podotknout, že při formalizaci procesů jsem vycházel především z obecného popisu problematiky správy IT služeb v oficiálních publikacích knihovny ITIL v3. Implementace daných procesů v reálném prostředí by nepochybně vyžadovala dodatečné přizpůsobení formalizovaných procesů specifickým podmínkám a potřebám konkrétní organizace.

Z pohledu dalšího vývoje práce se nabízí několik variant. Jednou z nich je porovnání a možnost koexistence rámce ITIL s dalšími standardy v oblasti ITSM, kterými jsou například COBIT [21], ASL [22] nebo MOF [23]. Další variantou je podrobné srovnání nejnovější verze knihovny s její předchozí verzí, která je v dnešní době stále aktuální v mnoha organizacích. Z praktického hlediska by mohl vývoj projektu pokračovat ve formalizaci ostatních procesů ITIL v3 a v případě reálné implementace těchto procesů v organizaci by bylo rovněž možné zabývat se jejich simulací.

7 Literatura

- [1] Procesní řízení IT služeb. *SystemOnLine*. [Online] [Citace: 2. únor 2010.] <http://www.systemonline.cz/sprava-it/procesni-rizeni-it-sluzeb.htm>.
- [2] Information Technology Infrastructure Library. *Wikipedia*. [Online] [Citace: 2. únor 2010.] http://cs.wikipedia.org/wiki/Information_Technology_Infrastructure_Library.
- [3] Normy jakosti řady ISO 9000. *Management jakosti*. [Online] [Citace: 2. únor 2010.] <http://normy.jakosti.cz/>.
- [4] A Short History of ITIL. *ITIL central*. [Online] [Citace: 2. únor 2010.] <http://itsm.fwtk.org/History.htm>.
- [5] **Grasseová, Monika, a další.** *Procesní řízení ve veřejném i soukromém sektoru*. Computer Press, 2008. 978-80-251-1987-7.
- [6] ITIL - Nejrozšířenější přístup k řízení informatiky. *SystemOnLine*. [Online] [Citace: 4. únor 2010.] <http://www.systemonline.cz/clanky/itil-nejrozsiरेnejsi-pristup-k-rizeni-informatiky.htm>.
- [7] ITIL & IT Service Management. *Empowered Networks*. [Online] [Citace: 31. leden 2010.] <http://www.empowerednetworks.com/approach/itil-and-itsm.aspx>.
- [8] **Taylor, Sharon, Iqbal, Majid a Nieves, Michael.** *ITIL: Service Strategy*. The Stationery Office, 2007. 9780113310456.
- [9] **Taylor, Sharon, Lloyd, Vernon a Rudd, Colin.** *ITIL: Service Design*. The Stationery Office, 2007. 9780113310470.
- [10] **Cartlidge, Alison, a další.** *An Introductory OverView of ITIL V3*. 1st ed. itSMF Ltd, 2007. 0-9551245-8-1.
- [11] **Taylor, Sharon, Lacy, Shirley a MacFarlane, Ivor.** *ITIL: Service Transition*. The Stationery Office, 2007. 9780113310487.
- [12] **Taylor, Sharon, Cannon, David a Wheeldon, David.** *ITIL: Service Operation*. The Stationery Office, 2007. 9780113310463.
- [13] **Taylor, Sharon, Case, Gary a Spalding, George.** *ITIL: Continual Service Improvement*. The Stationery Office, 2007. 9780113310494.
- [14] **Weske, Mathias.** *Business Process Management: Concepts, Languages, Architectures*. Berlin Heidelberg : Springer-Verlag, 1998. 978-3-540-73521-2.
- [15] **van der Aalst, Will, van Hee, Kees M. a Houben, Geert-Jan.** Modelling and analysing workflow using a Petri-net based approach. [Online] 1994. [Citace: 19. březen 2010.] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.37.7958&rep=rep1&type=pdf>.
- [16] **van der Aalst, Will.** The Application of Petri Nets to Workflow Management. [Online] 1998. [Citace: 21. březen 2010.] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.37.8232&rep=rep1&type=pdf>.
- [17] —. Petri-net-based Workflow Management Software. [Online] 1996. [Citace: 22. březen 2010.] <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.57.2932&rep=rep1&type=pdf>.

- [18] **Desel, Jörg, Reisig, Wolfgang a Rosenberg, Grzegorz.** *Lectures on concurrency and Petri nets: advances in Petri nets*. Berlin Heidelberg : Springer-Verlag, 2004. 3-540-22261-8.
- [19] **Vondrák, Ivo.** Metody byznys modelování: pro kombinované a distanční studium. [Online] 2004. [Citace: 21. březen 2010.]
http://vondrak.cs.vsb.cz/download/Metody_byznys_modelovani.pdf.
- [20] —. *Business Process Studio*. [Online] 3.0, 1998-2000. [Citace: 18. březen 2010.]
http://vondrak.cs.vsb.cz/download/bpstudio_eval/manual.pdf.
- [21] COBIT. *Wikipedia*. [Online] [Citace: 15. duben 2010.]
<http://en.wikipedia.org/wiki/COBIT>.
- [22] Application Services Library. *Wikipedia*. [Online] [Citace: 15. duben 2010.]
http://en.wikipedia.org/wiki/Application_Services_Library.
- [23] Microsoft Operations Framework. *Wikipedia*. [Online] [Citace: 2010. duben 15.]
http://en.wikipedia.org/wiki/Microsoft_Operations_Framework.

8 Seznam příloh

1. **Modely procesu Incident Management** – nachází se na přiloženém CD v adresáři */Modely/IncidentManagement*
2. **Modely procesu Problem Management** – nachází se na přiloženém CD v adresáři */Modely/ProblemManagement*
3. **Modely procesu Change Management** – nachází se na přiloženém CD v adresáři */Modely/ChangeManagement*